DOCUMENT RESUME

ED 421 996 IR 019 030

AUTHOR	Szuba, Tom
TITLE	Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security.
INSTITUTION	National Center for Education Statistics (ED), Washington, DC.; National Postsecondary Education Cooperative.; National Forum on Education Statistics.
REPORT NO	NCES-98-297
PUB DATE	1998-00-00
NOTE	153p.
PUB TYPE	Guides - Non-Classroom (055)
EDRS PRICE	MF01/PC07 Plus Postage.
DESCRIPTORS	Access to Information; Computer Networks; *Computer Security; Computer Software; *Educational Administration; *Educational Equipment; Educational Planning; Educational Policy; *Educational Technology; Elementary Secondary Education; Information Management; Internet; Needs Assessment; Online Systems; Program Implementation; Safety; Strategic Planning

ABSTRACT

This guide was developed specifically for educational administrators at the building, campus, district, system, and state levels, and is meant to serve as a framework to help them better understand why and how to effectively secure their organization's information, software, and computer and networking equipment. This document is organized into 10 chapters/content areas: (1) Why Information Security in Education?; (2) Assessing Your Needs (Risk Assessment); (3) Security Policy: Development and Implementation; (4) Security Management; (5) Protecting Your System: Physical Security; (6) Protecting Your System: Information Security; (7) Protecting Your System: Software Security; (8) Protecting Your System: User Access Security; (9) Protecting Your System: Network (Internet) Security; and (10) Training: A Necessary Investment in Staff. Each chapter includes: an overview, commonly asked questions, anecdotes illustrating real-world relevance, security guidelines (actual recommendations), and a summary checklist of "things to do" (based on the guidelines). Key points about the development and implementation of effective information security policies are conveyed throughout the document. A glossary, index, and appendices containing additional resources about computing, a FERPA Fact Sheet, related NCES publications, sample acceptable use agreements, a bibliography and selected reference materials and citations are included. (AEF)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED 421 996

Safeguarding YOUR Technology

Practical Guidelines for Electronic Education Information Security

BEST COPY AVAILABLE

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

- ☐ This document has been reproduced as received from the person or organization originating it.
- ☐ Minor changes have been made to improve reproduction quality.
- • Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

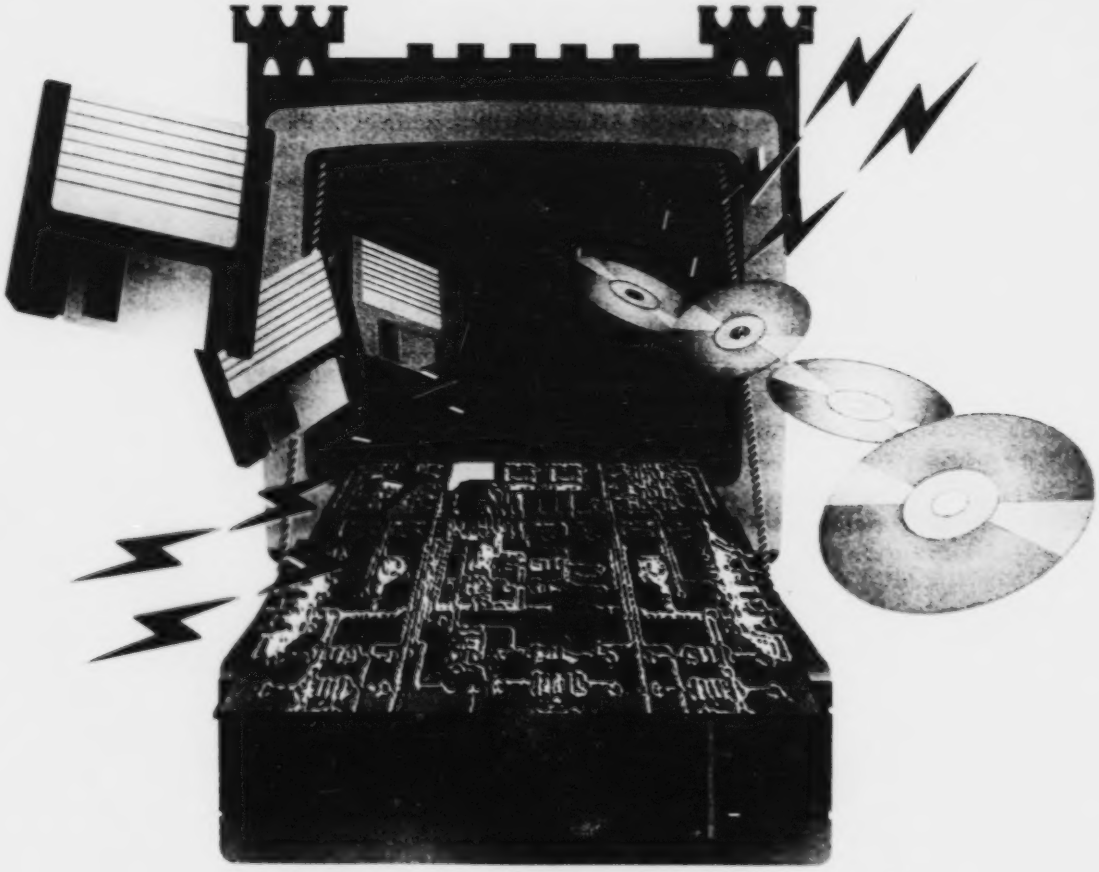
IR019030

National Center for Education Statistics

National Cooperative Education Statistics System

National Forum on Education Statistics

Safeguarding YOUR Technology



Practical Guidelines for Electronic Education Information Security

Tom Szuba, principal author
Technology & Security Task Force, National Forum on Education Statistics
Steve King, chairman

National Center for Education Statistics

National Cooperative Education Statistics System

National Forum on Education Statistics

3

U.S. Department of Education
Richard W. Riley
Secretary

Office of Educational Research and Improvement
C. Kent McGuire
Assistant Secretary

National Center for Education Statistics
Pascal D. Forgione, Jr.
Commissioner

The National Center for Education Statistics (NCES) is the primary federal entity for collecting, analyzing, and reporting data related to education in the United States and other nations. It fulfills a congressional mandate to collect, collate, analyze, and report full and complete statistics on the condition of education in the United States; conduct and publish reports and specialized analyses of the meaning and significance of such statistics; assist state and local education agencies in improving their statistical systems; and review and report on education activities in foreign countries.

NCES activities are designed to address high priority education data needs; provide consistent, reliable, complete, and accurate indicators of education status and trends; and report timely, useful, and high quality data to the U.S. Department of Education, the Congress, the states, other education policymakers, practitioners, data users, and the general public.

We strive to make our products available in a variety of formats and in language that is appropriate to a variety of audiences. You, as our customer, are the best judge of our success in communicating information effectively. If you have any comments or suggestions about this or any other NCES product or report, we would like to hear from you. Please direct your comments to:

National Center for Education Statistics
Office of Educational Research and Improvement
U.S. Department of Education
555 New Jersey Avenue, NW
Washington, DC 20208-5574

September 1998

The NCES World Wide Web Home Page is
http://nces.ed.gov

U.S. Department of Education, National Center for Education Statistics. *Safeguarding Your Technology.* NCES 98-297, Washington, DC: 1998.

Contact:
Gerald Malitz
(202) 219-1364

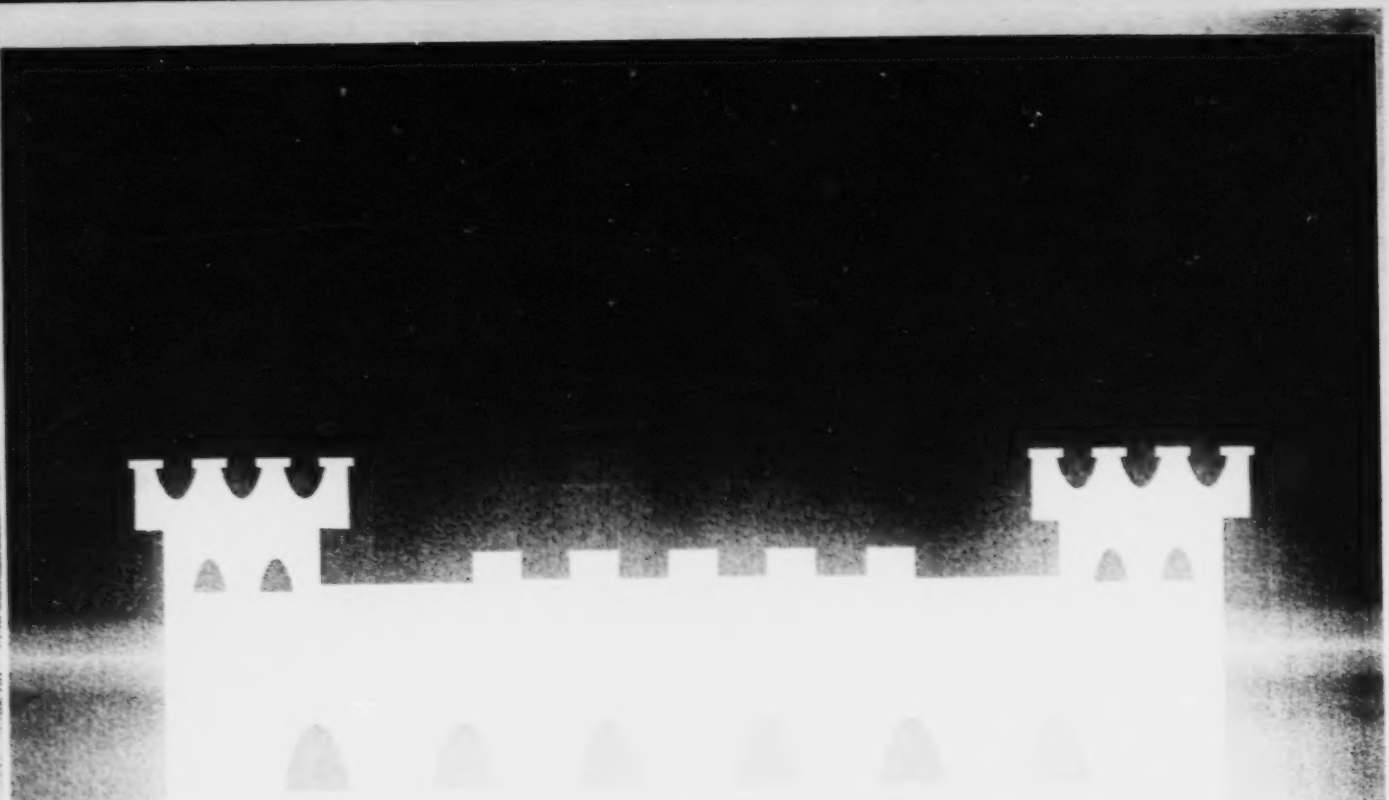


Table of Contents

Acknowledgments iv

Executive Summary vii

Preface ix

Chapter 1 - Why Information Security in Education? 1

A Brief History of Security in Education 2
What's at Risk? 3
Why Administrators Should Read These Guidelines 4
Document Framework 6
A Final Word on Considering Security Issues 7
Introductory Security Checklist 8

Chapter 2 - Assessing Your Needs 11

Introduction to Risk Assessment 11
Commonly Asked Questions 13
Components of Risk 14
Assets 14
Threats 15
Vulnerabilities 16
Countermeasures 16
Dealing with Risk 17
Guidelines for Risk Assessment 17
The Players: It's a Team Effort 18
Timing: First Things First 19
Take Stock in What You Have and What It's Worth 19
Identify Your Potential Threats and Vulnerabilities 20
Think Through Your Defensive Options 22
Make Informed Decisions 23
Closing Thoughts on Risk Assessment 24
Risk Assessment Checklist 24

Chapter 3 - Security Policy: Development and Implementation 27

Why Do You Need a Security Policy? 28
Commonly Asked Questions 28
How to Develop Policy 29
Getting Perspective 29
What to Include 30
Writing with Proper Tone 30

From the Board Room to the Break Room: Implementing Security Policy . . . 31
Personnel Issues . . . 33
A Special Note on Outsiders . . . 33
Closing Thoughts on Policy . . . 34
Policy Development and Implementation Checklist . . . 34

Chapter 4 - Security Management . . . 37

Introduction to Security Management . . . 37
Commonly Asked Questions . . . 38
Nurturing Support within the Organization . . . 39
Garnering Administrator Support . . . 39
Ensuring User Support . . . 40
Planning for the Unexpected . . . 40
Security Breach Response Planning . . . 41
Contingency Planning . . . 42
Testing and Review . . . 45
Implementation and Day-to-Day Maintenance . . . 47
Backups . . . 47
Virus Protection . . . 49
Software Updates . . . 49
User Account Management . . . 50
System Use Monitoring . . . 50
Security Management Checklist . . . 52

Chapter 5 - Protecting Your System: Physical Security . . . 55

Introduction to Physical Security . . . 55
Commonly Asked Questions . . . 55
Policy Issues . . . 56
Physical Security Countermeasures . . . 57
Physical Security Checklist . . . 63

Chapter 6 - Protecting Your System: Information Security . . . 67

Introduction to Information Security . . . 67
Commonly Asked Questions . . . 67
Policy Issues . . . 68
Information Security Countermeasures . . . 69
Information Security Checklist . . . 74

Chapter 7 - Protecting Your System: Software Security . . . 77

Introduction to Software Security . . . 77
Commonly Asked Questions . . . 77
Policy Issues . . . 78
Software Security Countermeasures . . . 78
Software Security Checklist . . . 83

Chapter 8 - Protecting Your System: User Access Security 85

Introduction to User Access Security 85
Commonly Asked Questions 86
Policy Issues 87
User Access Security Countermeasures 87
User Access Security Checklist 92

Chapter 9 - Protecting Your System: Network (Internet) Security 97

Introduction to Network Security 97
Commonly Asked Questions 97
Policy Issues 99
Network Security Countermeasures 100
Closing Thoughts on Network Security 102
Network Security Checklist 103

Chapter 10 - Training: A Necessary Investment in Staff 105

Introduction to Training 105
Commonly Asked Questions 107
Targeting Training Efforts 107
Training Goals 109
A Sample Training Outline 110
Training Frequency 112
Closing Thoughts on Security Training 113
Security Training Checklist 113

Appendices

A. Additional Resources about Computing 115
B. FERPA Fact Sheet 116
C. Related NCES Publications 117
D. Sample Acceptable Use Agreements 118
E. Bibliography and Selected Reference Materials 123
F. Citations 125

Glossary 126

Index 140

Acknowledgments

This document was developed through the National Cooperative Education Statistics System and funded by the National Center for Education Statistics (NCES) of the U.S. Department of Education. A Task Force of the National Forum on Education Statistics conceptualized and oversaw the development of this document. The task force, whose members represent all levels of the education system, wishes to acknowledge the efforts of many individuals who also contributed to the development of this document.

Scott Williams of the U.S. Bureau of the Census provided the task force with an early overview of computer security considerations. He served as an excellent resource to the task force and helped it to focus its efforts.

After task force members each contributed a draft chapter of the document, the separate files were consolidated and edited into a single document. This initial draft was then distributed to selected reviewers in California, Iowa, and West Virginia. A subgroup of the task force met with these reviewers in focused interview sessions. These site visits provided a "reality check" from users with a broad range of training, expertise, and responsibility. The reviewers came from elementary, secondary, and post-secondary environments; instructional and administrative settings; and private and public schools. Their contributions were constructive and substantial. The document was improved considerably after being revised based on feedback received during these site visits.

Coordinating these site visits was a significant task in itself. Each state coordinator solicited and organized reviewers, assisted in the distribution of drafts, and facilitated meeting times and places. The task force extends its deep appreciation to Steve Boal (Iowa Department of Education), Jan Volkoff (California Department of Education), and Nancy Walker (West Virginia Department of Education) for serving in this capacity in their states.

The task force also wishes to extend its deepest appreciation to Tom Szuba, project consultant and coordinator, for his efforts in compiling the various submissions from the task force members and revising them into a unified document. He did an exceptional job of merging divergent content and making technical information accessible—it was one of the strongest points of praise from the site visit reviewers. He also had the difficult job of keeping the task force on task and on timeline, a duty he managed well.

Finally, the task force wishes to thank Gerald Malitz of NCES and Oona Cheung of the Council of Chief State School Officers for their assistance with the overall management and development of this project.

The following is a list of task force members:

Steven King (Chairperson)
Wyoming Department of Education

Marc Anderberg
Texas SOICC

Oona Cheung
Council of Chief State School Officers

Paul Gammill
Prince George's County Public Schools (Maryland)

Roy Herrold
Central Susquehanna (PA) Intermediate Unit

Gerald Malitz
National Center for Education Statistics

Cheryl Purvis
Nevada Department of Education

Andy Rogers
Los Angeles (CA) Unified School District

Tom Saka
Hawaii Department of Education

Jeff Stowe
Arizona Department of Education

Judy Thompson
Connecticut Department of Education

Jim Villars
Osseo (MN) Area Schools

Duane Whitfield
Florida Department of Education

Site Visits

After a draft of this document was completed, site visits were scheduled to have the document reviewed for content, format, and utility. The following is a list of site visit participants who served as reviewers:

California Department of Education

Lynn Baugher, Administrator
School Business Services

Karl Scheff, Consultant
Education Demographics

Wayne Shimizu, Consultant
School Business Services

Jan Volkoff, Consultant
(State Site Visit Coordinator)

California State Senate

Tanya Lieberman, Consultant
Budget Committee

Belle Vista High School (CA)

Peggy Desmond, Vice Principal

Jim Reidt, Principal

Fallbrook Union (CA) Elementary School District

Allan Roth, Director of Student Programs

Gateway (CA) Unified School District

Midge Kenyon, Director of Information Resources

Grant Joint Union HS District (CA)

Frank Fish, Director of Information Systems

Los Angeles County (CA) Office of Education

Nancy Kraus, Director
Division of Educational Support Services

James K. McGill, Assistant Director
Network Engineering and Applications

San Francisco (CA) Unified School District

Catherine Secour, District Registrar

San Juan Unified (CA) School District

Errol Belt, Network and Technology Manager

Dan O'Halloran, Networking Specialist

Mike Parks, Custodian of Pupil Records

Santa Clara County (CA) Office of Education

Ruthellen Dickinson, Systems Coordinator

Shasta County (CA) Office of Education

Jim Demarco, Technology Coordinator

Van Wilkinson, Development and Technology Director

Computer and Network Consulting

John McBrearty

West Ed

Kathryn Bangert, Information Systems Analyst

L. Russ Brawn, Project Manager

Graham Charles, Information Systems Analyst

Steve Mills, Senior Program Associate

Janice Schafer, Research Associate

Iowa State Department of Education

David J. Alvord, Chief
Bureau of Planning, Research, and Evaluation

Steve Boal, Consultant
Bureau of Planning, Research, and Evaluation
(State Site Visit Coordinator)

Greg Fay, Network Manager

David Krieger, Data Processing Manager

Lee Tack, Administrator
Division of Financial and Information Services

Kirkwood Community College (IA)

Rick Anderson, Director
Business Services

Tina M. Herb, Network Computing Director

Patrick Murphy, Executive Director
Computer Information Services

Tom Sabotta, Director
Enrollment Services/Institutional Research

Roger Seamands, System Programmer

Doris Steffen, Computer Operations Coordinator

Des Moines (IA) School District

Linda Adrianse, Pupil Services Coordinator
Lincoln High School

Fran Blasberg, Principal
Wright Elementary

Carol Gustafson, Student Accounting Specialist
Des Moines School District

Waukee (IA) School District

Bruce Kimpston, Dean
Waukee High School

Denise Krefting, Technology Director
Waukee School District

Bernie Van Roekel, Principal
Waukee High School

Dave Wilkerson, Director of Instructional Services
Waukee School District

University of Iowa

Jerald W. Dallum, Registrar

Cindy Dayton, EDI Administrator

Karen Knight, Associate Director of Admissions

Doug Lee, Provost Officer

Sue Nickels, ITS Contingency Planning Coordinator

Catherine Pietrzyk, Associate Registrar

Dennis Preslicka, ITS Customer Relations

Don Szeszycki, Provost Officer

West Virginia Department of Education

Marshall Patton, Student Software Support Manager

Nancy Walker, WVEIS Executive Director
(State Site Visit Coordinator)

Doris White, Data Coordinator

University of Charleston (WV)

Alan Belcher, Coordinator of Academic Technology

Craig Timmons, Director of Computing

Connie Young, Registrar

Berkeley County (WV) Schools

Nancy Kilmon, Director
Research and Technology

Jackson County (WV) Schools

Ronald E. Ray, Secondary Director

Kanawha County (WV) Schools

Nancy Baldwin, Computer Technician

Rebecca Butler, Area Technology Teacher

Bill Carter, Network Technologist

Steven Hinchman, Computer Technician

Dale A. Nichols, Area Technology Teacher

Mercer County (WV) Schools

Nancy L. Moore, WVEIS County Contact

David S. Palmer, WVEIS County Coordinator

Garry Taylor, Supervisor

Mingo County (WV) Schools

Nell Hatfield, Certification/Media Specialist

Summers County (WV) Schools

Richard Lawrence, Technical Coordinator

Wood County (WV) Schools

Robert Mathews, Director
Technical and Media Services

Belle Elementary School (WV)

John Eagle, Principal

Brooke High School (WV)

Donald J. Hendon, WVEIS Coordinator

Charleston Catholic High School (WV)

Deborah Sullivan, Principal

Clendenin Middle School (WV)

Cathy Bennett, Principal

Hampshire High School (WV)

Scott Cather, Assistant Principal

Hurricane Middle School (WV)

Richard Grim, Assistant Principal

Richmond Elementary School (WV)

John Cummings, Principal

South Charleston High School (WV)

Clifford Cunnigham, Curriculum Supervisor

St. Albans High School (WV)

Carl Garner, Vice Principal

Tucker Valley Elementary/Middle School (WV)

Michael W. Kessinger, Principal

Tucker Valley High School (WV)

Rose T. Kessinger, Principal

Design and creative direction:
The Creative Shop, Bethesda, MD

Executive Summary

Accessing, manipulating, and sharing information electronically has proven time and time again to be a cost-effective way of getting things done. Thus, it isn't surprising that many schools, school districts, state education agencies, and colleges and universities now use technology to manage student, staff, and administrative records. Unfortunately, safeguarding electronic information is not as straightforward as simply assigning a technical staff person to verify that the "system" is protected. It requires that top-level administrators invest time and expertise into the development of a well-conceived, comprehensive, and customized security policy. This policy must then be applied appropriately throughout the entire organization, which again requires the commitment and authority of top-level administrators. After all, while technical staffers might be responsible to top-level educational administrators for information technology security, the top-level administrators are in turn responsible to the greater public.

What's at Stake?

1. *Computer and networking equipment (including both hardware and software)* used for both instructional and administrative purposes
2. *Vital administrative information* education organizations must use to operate efficiently and fulfill their mission effectively (e.g., class management information, password archives, and financial records)
3. *Confidential student and staff information* education organizations maintain and are responsible for

Most people see the necessity of securing computer and networking equipment. Machines cost money, and therefore have value unto themselves. But if you take a moment to consider why organizations are so willing to spend large amounts of money on technology—to store, access, and transmit information—the value of the information becomes more apparent. After all, it makes no sense to spend vast amounts of limited resources on a system for processing information unless the information itself is of value. And because information has become so useful, it's not only the hardware and software that demand protection, but also the data. When information is lost, damaged, or otherwise unavailable when needed, it can have a serious effect on the day-to-day operations of an education organization. And when the information at risk is an individual student record, the consequences can be even more serious. What would be the damage, for example, if student report card files were modified inappropriately or confidential student aptitude scores were revealed improperly?

> *Would the cost of such a security breach be $2,000 to rekey information? Or $20,000 to readminister tests? Perhaps $200,000 in settling legal suits? How about $2,000,000 in lost technology funding when lawmakers become fearful of entrusting private information about their constituents' children to record systems that are perceived to be unsafe?*

You should not, however, conclude that the repercussions of mishandling information are limited to simple dollars and cents. Failing to secure confidential information can carry other consequences as well. Educational staff have not only an ethical responsibility to protect confidential information about students and their parents, but also a legal obligation to do so. Many states and localities have enacted laws and regulations to protect a student's right to privacy. So, too, has the federal government—the Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal guarantee of the privacy of educational records for students and their parents.

Educational administrators are well trained and knowledgeable about the protection of education records in a paper world. But as information management becomes more and more technologically advanced, they must also be able to protect electronic information and the software and hardware used to manage it. What makes the issue of information security more difficult is that many, if not most, educational administrators do not have the technical expertise or, given their other vitally important duties, the time to devote to single-handedly developing, implementing, and monitoring information security policies and procedures for their organizations. Nonetheless, the responsibility for both meeting the public's demands for accountability and adequately securing information, software, and equipment is inescapable for top administrators. Like it or not, it comes with the job. And that is why this document has been developed.

Unlike other resources on electronic information security, this guide has been developed specifically for educational administrators at the building, campus, district, system, and state levels (e.g., school principals, district superintendents, state chiefs, college deans, and their assistants). It is meant to serve as a framework to help them better understand why, and how, to effectively secure their organization's information, software, and computer and networking equipment. Because this intended audience has in most cases been trained to manage education organizations and not computer systems, the document is written in non-technical language and emphasizes a step-by-step approach to protecting education information in a technology-based system, regardless of computer or network type and technical savvy. Since only the reader understands his or her organization, its needs, capabilities, limitations, and unique circumstances, the guidelines are presented as well-researched recommendations (*not* canned solutions) for developing security policies that are *customized to meet each organization's specific needs.*

The document is organized into ten content areas (chapters): (1) Why Information Security in Education? (An Introduction), (2) Assessing Your Needs (Risk Assessment), (3) Security Policy (Development and Implementation), (4) Security Management, (5) Physical Security, (6) Information Security, (7) Software Security, (8) User Access Security, (9) Network (Internet) Security, and (10) Training (A *Necessary* Investment in Staff).

Each chapter includes:

- An overview
- Commonly asked questions
- Anecdotes illustrating real-world relevance
- Security guidelines (actual recommendations)
- A summary checklist of "things to do" (based on the guidelines)

Key points about the development and implementation of effective information security policies that are conveyed throughout the document include:

- Successful information security policy requires the leadership, commitment, and active participation of top-level educational administrators.
- Information security initiatives must be customized to meet the unique needs of the organization.
- Effective information security is the result of a process of identifying an organization's valued information, software, and computer and networking equipment; considering the range of potential risks to those resources; tailoring security policy to those specific conditions; and ensuring that policy is not only developed properly but also implemented reliably.
- Critical information security strategies rely primarily upon appropriate conduct on the part of personnel, and secondarily on the use of technological solutions.

Above all, this document hopes to convey that increasing information security is both a necessary and achievable task. It is the prudent thing to do for organizations and the right thing to do for students, parents, staff, and communities. These practical guidelines provide direction for those top-level educational administrators who must lead the effort.

Preface

These guidelines are written to help educational administrators and staff at the building, campus, district, and state levels better understand why and how to effectively secure their organization's sensitive information, critical systems, and computer equipment.

This document is:

- Concerned primarily with information technology security as it relates to the privacy and confidentiality of education information
- Organized so as to walk policy-makers through the steps of developing and implementing sound security policy that is tailored to meet the needs of their individual organizations
- Focused on both technical and procedural requirements (i.e., both computer-related and staff-related issues)
- Presented as a set of recommended guidelines
- Also available electronically at the National Center for Education Statistics' website at http://nces.ed.gov

Formatting Conventions

While all of the information in this guide is important to an educational administrator who is developing and implementing security policy in his or her organization, some points stand out in particular. To better emphasize these points, a few symbols are used throughout the document.

Look for These Symbols

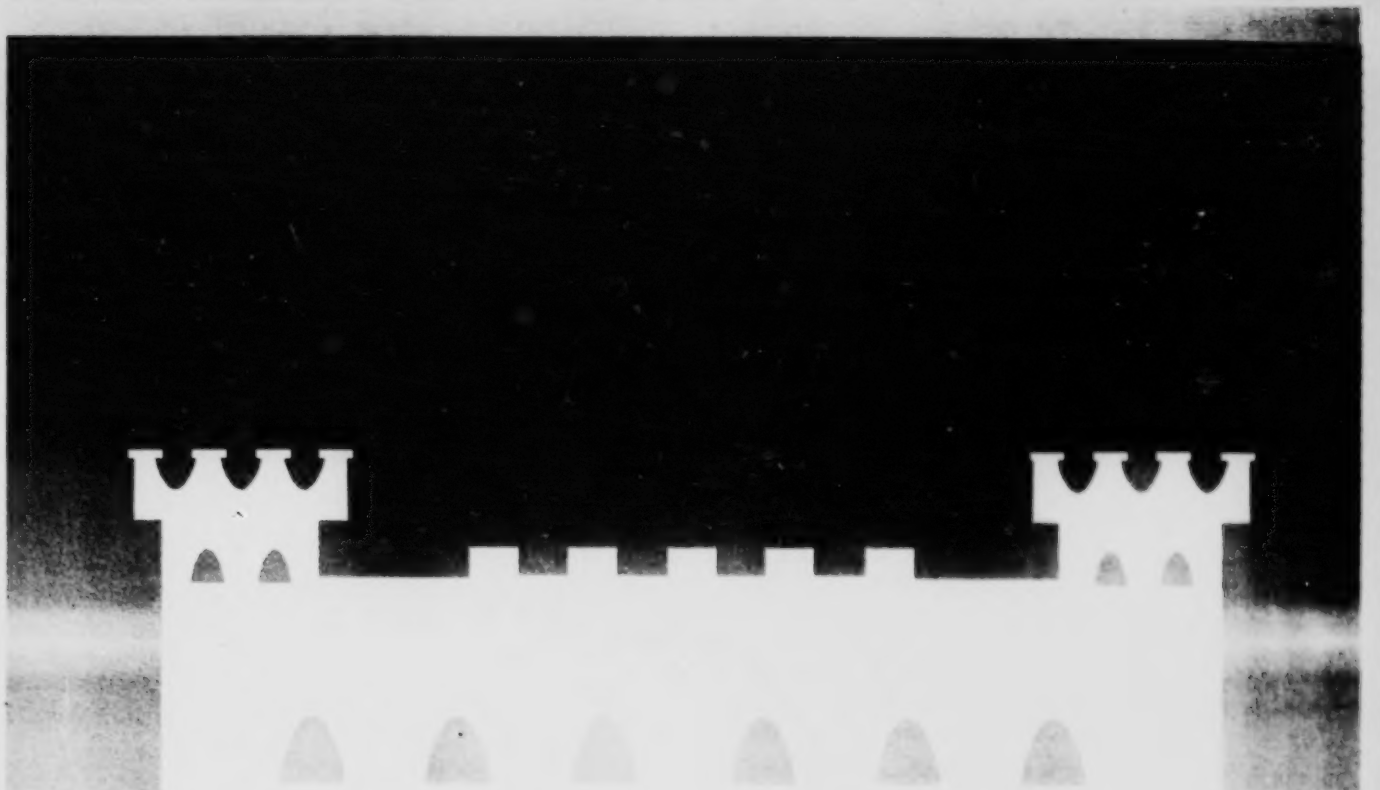
A castle denotes something that is or should be done.

A bomb denotes something that is not or should not be done.

Lightning bolts denote an important point, so read closely!

Notice, for example, that the "lightning bolts" in the left margin below alert readers that they are permitted to modify, customize, and reproduce any part of this document. Also included, where appropriate, are superscript numbers to denote resource citations as listed in Appendix F. Lastly, terms that are defined in the glossary are in **bold** the first time they appear in each chapter.

Note that users are expressly permitted to modify, customize, and reproduce any part of this document.



CHAPTER 1

Why Information Security in Education?

CHAPTER 1 IN A NUTSHELL:

A Brief History of Security in Education	pg 2
What's at Risk?	pg 3
Why Administrators Should Read These Guidelines	pg 4
Document Framework	pg 6
A Final Word on Considering Security Issues	pg 7
Introductory Security Checklist	pg 8

It Really Happens!

Hillary Johnson saw the headline in the Sunday paper. It just couldn't be true, could it? She read further and realized how bad the situation really was:

Fire Ravages School Warehouse

Decades Worth of Records Destroyed

Fire raged through the warehouse, burning school records from as far back as the early 1950s. In a prepared statement, the Superintendent of Schools acknowledged that "many, if not all, files were destroyed in the blaze. This is a real tragedy for our community. People refer to their school records for the rest of their lives. Now, for many of our former students, there simply is no record of their time in county schools." As recently as last spring, the School Board debated the necessity of duplicating archived student records electronically, but a vote on the proposal was postponed and not rescheduled for consideration until next month.

Hillary was beside herself with worry. She had very definitely been told in her first interview that she needed to bring proof of high school graduation when she went to meet with the supervisor. What would they do when she told them that she couldn't get a copy of her school records? She really needed that job. Would they understand her predicament, or just hire the person who had all of the paperwork?

Unfortunately, Hillary wasn't the only one upset at the loss of academic history. Amanda Chang was equally concerned when she saw the story. Five years after finishing high school, she was finally ready to apply to college, but knew that doing so required a high school transcript as a part of the application process. Did this mean that maybe she really wasn't meant to go to college after all?

But poor Chet Wilcox was perhaps most distraught of all. He had been planning to use his school records to verify his age for retirement. What would he do if he couldn't prove that he qualified for benefits?

As the Superintendent of Schools acknowledged in her statement after the fire, for countless numbers of people, school records are not just "memories of days gone by," but vitally important documentation of their life experiences. They retain meaning and significance long after high school graduation and really do affect people's lives.

While such an article may only be anecdotal in this instance, the point it illustrates is real: school records are not just important for administrative reasons—they affect people for the rest of their lives, as they are used to apply for employment, for admission to higher education, and, in some cases, even retirement benefits.

A Brief History of Security in Education

Robbery is illegal, but people still find it prudent to lock doors and close windows in their homes; so too must we lock up our information **systems.** Like people who lock their doors, schools have always been concerned about protecting their valued resources, including **confidential information** contained in student and staff records.

Before the widespread use of **computers,** educational administrators were responsible for safeguarding paper records that were often kept in filing cabinets. The cabinets were probably locked in the administrator's office, and were perhaps themselves locked. Maybe the administrator held the only key; at most, a secretary was given a copy in case of unforeseen problems. In recent years, however, most education organizations have joined other public and private sector entities in adopting technology as the primary means by which they organize and **access** information. Sharing **information** via computers and **networks** has proven time and time again to be a cost-effective way of getting things done. In fact, today's society relies upon computers now more than ever and will more than likely continue to increase its use of technology. As the saying goes, information is power. In schools, it is the power to make the entire educational process more efficient. Information about students, staff, courses, programs, facilities, and fiscal activities is collected and maintained so that schools can effectively coordinate services offered to students, measure learning progress, assign and monitor staff responsibilities and resource use, and provide other valued services to their communities.

There are numerous legitimate reasons for collecting, using, and sharing education information appropriately.

But as new as technology is to the workplace, its application is an extension of the way schools have always conducted their business. While computers and networks contribute to the efficiency of educational record-keeping, **data** access, and use, they have not changed the reasons schools need to maintain, share, and use student and staff information. The education community has always required these types of information to carry out its mission to instruct students.

Technology is simply a tool for accomplishing necessary tasks more efficiently.

Although it may be fitting to discuss analogies between paper **files** in wooden cabinets and electronic files on **hard drives** or 3½-inch **diskettes,** there are significant differences in the specific processes required to maintain appropriate security in the age of computer networking. With the flip of a switch, information can be damaged irreparably. With the careless turn of your head, a pocket-sized **disk** containing thousands of records can disappear. And with the connection of a single wire, sensitive material can be shared with millions of users.

While these scenarios may seem foreboding and even scary, they are only part of the story—and, in fact, a small part—because by flipping a different switch, properly storing disks, and connecting the right wires, information stored on school computers and networks can be secured more safely than any paper file in any administrator's office filing cabinet, whether locked by deadbolt or protected by an armed guard.

The same technology that can be the source of so much concern when in the hands of untrained users can actually be used to protect information more securely than ever before imaginable if it is used wisely.

What's at Risk?

Most people see the necessity of securing computer equipment. Machines cost money and therefore have value unto themselves. But if you take a moment to consider why organizations are so willing to spend large amounts of money on their computer systems—to store, access, and transmit information—the value of that information becomes more apparent. After all, it makes no sense to spend vast amounts of limited resources on equipment for processing information unless the information itself is of value. And because information has become so useful, it's not only the equipment that demands protection, but also the data. In the education community, information about students, staff, and other resources is far more valuable to the operation of school buildings, campuses, and district and state education agencies than even the most costly equipment. How could it be so?

For starters, education data can represent years' worth of investment in collection and maintenance activities, and may be irreplaceable as an **asset.** What would happen, for example, if a school "lost" grade information and was unable to calculate cumulative grade point averages for its graduating class?

In the larger scheme, education information is often considered to be confidential by its very nature—that is, certain types of **sensitive information** (in particular individually identifiable student and staff records) must, by law, be protected from all parties who do not have a verifiable ***need-to-know.*** In addition to numerous state and local laws designed to preserve the confidentiality of education records, the Family Education Rights and Privacy Act of 1974 (FERPA) (see Appendix B) is a federal law designed specifically to protect the privacy of a student's education record. It applies to all schools that receive funding under an applicable program of the U.S. Department of Education, and is but one example of legislation enacted specifically to protect confidential student information maintained in education record systems.

"Need-to-know" refers to a legitimate educational reason for accessing confidential student records.

Another document published by the National Forum on Education Statistics, *Protecting the Privacy of Student Records: Guidelines for Education Agencies,* describes *what* and *why* specific types of information about students and their families are considered to be confidential and clarifies relevant laws governing proper and improper release of such records. This document, in turn, explains *how* to satisfy these requirements.

Since the institution is ultimately responsible for the integrity and security of its data, the organization and its management need to take active steps to ensure that valuable equipment and, more importantly, information (such as private student and staff records) are being adequately protected. If an education organization fails to protect its confidential information in a manner that satisfies "standards of due care" and "reasonable safeguards," it opens itself to a host of potential problems from allegations of negligence and incompetence, to law suits charging "computer malpractice," and forfeiture of insurance claims due to "preventable losses."[1] In addition to the legal ramifications of privacy violations, the potentially priceless asset of public confidence is also at **risk.** School boards, legislatures, and other governing bodies often look quite

unfavorably upon institutions and staff responsible for upsetting public confidence in the government's need to collect, maintain, and use information about its constituency. And the public might justifiably lose confidence if a list of student aptitude scores was accessed improperly or a mischievous student managed to modify report cards or attendance data.

Why Administrators Should Read These Guidelines

What makes the issue of information security more difficult, however, is that many, if not most, education administrators do not have the technical expertise nor, given their other vitally important duties, sufficient time to devote to single-handedly developing, implementing, and monitoring information security policies and procedures within their organizations. Nonetheless, to paraphrase President Harry Truman, it is upon the heads of those very education administrators that "the buck stops." Responsibility for both meeting the public's demands for accountability and securing sensitive information is inescapable for an education institution's chief administrative officer. Like it or not, it comes with the job. And that is why this document has been written.

Document Purpose and Audience

These guidelines are written to help educational administrators and staff at the building, campus, district, and state levels better understand why and how to effectively secure their organization's sensitive information, critical systems, and computer and networking equipment.

Because top educational administrators are ultimately responsible for information security, they must develop a sufficient understanding of sound security strategies and how they can be realized through organizational policy.

The intent of this document is to provide basic and timeless guidance to decision-makers by identifying factors that should be taken into consideration when (not if) they develop security strategies and policies to meet their organization's particular conditions and local circumstances. It is designed specifically to help educational staff as they endeavor to walk the fine line between keeping education data secure and yet at the same time available to authorized persons with legitimate purposes. Because the technical methods for securing digital data lie outside the training and expertise of most educational administrators, these guidelines (which are exactly that—well-researched recommendations rather than canned solutions) are written in non-technical language that is specifically tailored to educators.

Although a key recommendation of this document is that each education organization designate a technically competent staff person (or hire a consultant) to manage data security operations, administrators cannot be content to otherwise disregard security issues entirely. While operational *authority* can and should be delegated to staff or contractors, the actual burden of *responsibility* cannot be lifted from the shoulders of chief administrators. That is why top educational administrators need to develop a sufficient understanding of information security and its related issues: so that they can judge whether their subordinates are acting

competently and thoroughly and can subsequently ascertain whether proposed policies and procedures will be adequate and effective. After all, each policy will still be implemented over the administrator's signature.

In a nutshell, this document ***is:***

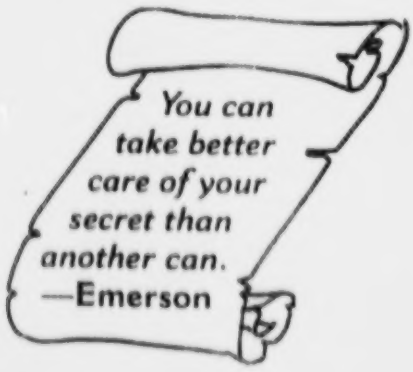
- An outgrowth of another National Forum on Education Statistics' document, *Protecting the Privacy of Student Records: Guidelines for Education Agencies*
- Concerned primarily with information technology security as it relates to the privacy and confidentiality of education information
- Designed specifically for use by education administrators and staff at the building, campus, district, and state levels
- Organized so as to walk policy-makers through the steps of developing and implementing sound **security policy** that is tailored to meet the needs of their individual organizations
- Focused on both technical and procedural requirements (i.e., both computer-related and staff-related issues)
- Presented as a set of recommended guidelines
- Also available electronically at the Web site for the National Center for Education Statistics (NCES) at http://nces.ed.gov

This document presents recommendations for securing information and equipment, but does *not* presume to dictate local policy.

This document ***is not:***

- An attempt to dictate policy (although it can and should serve as a guide to policy-makers as they consider their policy options and needs)
- Focused on a high-end discussion of security issues that requires readers to have advanced knowledge of technology issues
- Presented as a manual of technical solutions for securing systems
- A source for specific **software** product recommendations

This document does not presume to dictate local policy because, among other reasons, the parties responsible for developing these guidelines have no authority to issue or enforce security policies to autonomous education institutions. Nor does the document endorse specific products or vendors of security devices. Given the rapid pace of change in this field, such endorsements might be rendered obsolete by emerging technologies even before they could be printed and distributed.



Document Framework

The document includes the following chapters:

Chapter 1 - Why Information Security in Education? Chapter 1 describes the document's purpose, scope, intended audience, and organization.

Chapter 2 - Assessing Your Needs. Chapter 2 discusses the necessity of assessing an organization's unique needs as the first step to developing a security plan. It includes a description of the various components of risk and an outline of steps necessary for effectively conducting a risk assessment.

Chapter 3 - Security Policy: Development and Implementation. Chapter 3 recommends procedures and practices that contribute to the development of effective security policy. It also presents a range of issues that demand consideration before policy is created.

Chapter 4 - Security Management. Chapter 4 discusses a security manager's role and numerous responsibilities, including generating organizational support from top to bottom, directing contingency planning, overseeing system testing and reviewing, and performing day-to-day administrative activities.

Chapter 5 - Protecting Your System: Physical Security. Chapter 5 examines potential threats and vulnerabilities to a system that are of a physical nature. Practices by which equipment and other assets can be secured from such risks, referred to as countermeasures, are recommended.

Chapter 6 - Protecting Your System: Information Security. Chapter 6 considers potential threats and vulnerabilities that are directly related to a system's information (the data). It focuses on maintaining information confidentiality, integrity, and availability, and recommends strategies for protecting information while in transmission, in use, and in storage.

Chapter 7 - Protecting Your System: Software Security. Chapter 7 focuses on potential threats to computer software and specific countermeasures to those threats and software-related vulnerabilities.

Chapter 8 - Protecting Your System: User Access Security. Chapter 8 details threats and vulnerabilities that are related to those people who actually use a system. It describes security strategies that can be used to allow, prevent, and monitor access to system information.

Chapter 9 - Protecting Your System: Network (Internet) Security. Chapter 9 recommends strategies for protecting your network when connecting to other networks, and for transmitting information over the Internet in a secure manner.

Chapter 10 - Training: A Necessary Investment in Staff. Chapter 10 emphasizes the necessity of appropriate staff training when trying to implement security policy in any organization. It describes normal and predictable staff training needs and includes a sample outline of a training program.

It also includes the following Appendices:

Appendix A. Additional Resources about Computing

Appendix B. FERPA Fact Sheet

Appendix C. Related NCES Publications

Appendix D. Sample Acceptable Use Agreements

Appendix E. Bibliography and Selected Reference Materials

Appendix F. Citations

Glossary

Index

Each chapter is organized in the same general way. Expect to find:

An Introduction—An overview of the topic
Commonly Asked Questions—Issues people often wonder about
It Really Happens—Anecdotal accounts of real-world relevance
Content Body—General information, guidelines, and rationale
Checklists—A summary of security guidelines

A Final Word on Considering Security Issues

Security involves more than keeping intruders out of confidential files. While an organization must certainly be aware of system **hackers** (unauthorized **users** who attempt to access a system and its information), it must more *regularly* deal with **threats** like failed hard drives, spilled coffee, and refrigerator magnets.

Most security concerns an organization must face are of a fairly regular nature. For example, the phrase "mean time between failures" is quite common in the computer sales industry. For non-statisticians, it refers to when (not if) every computer disk you own will fail. Planning to deal with this eventuality is not an exercise in the theoretical!

Remember, however, that the goal of system security is not to put all of your organization's confidential records into an entry-proof vault that even authorized users have difficulty accessing. If that was the case, locking your keys in the car would be an effective security strategy for protecting the vehicle—you can be pretty certain that no one else can get into your car if even you, the owner, are unable to do so. Rather, the **goal of security** is to protect information and the system without unnecessarily limiting its utility. The system shouldn't be so secure that authorized users can't get to the data they need to do their jobs. After all, the only reason you bother to maintain such information in the first place is so that it can be used to help better serve your students.

At the same time, however, unauthorized access, especially to **critical systems** and sensitive information, must be prevented. Because of this contradiction, no system, be it electronic or paper, will ever be entirely secure, but the ideal of developing and maintaining a **"trusted system"** is realistic nonetheless, and should be the goal of every educational administrator.

To approach this goal, top-level decision-makers must be involved in any organization's attempt to establish sound information security policy and procedures. Although at times the prospect of such an endeavor may seem somewhat daunting, especially to a person who in all probability doesn't have technical training, it must be undertaken all the same. Simply by reading this document, educational administrators will be better prepared to grapple with both the general principles of security and those that are perhaps more unique to their own situations. But despite the specific guidelines that follow throughout this document, policy-makers must understand that in order to successfully institute security practices within an organization, the following overarching prerequisites must first be met:[2]

- *Senior* management must provide strong outward support.
- A single, *empowered* staff member must be made specifically responsible for security initiatives (and have the time needed for testing, monitoring, and other activities designed to provide feedback on the system).
- Employees must be educated through *well-conceived training programs.*
- *All* employees must participate at *all* times.

The bottom line is that if, as an educational administrator, you are prepared to commit to these requirements and make the effort to educate yourself on the issues affecting information security, protecting your organization's resources more effectively becomes entirely possible. By developing and implementing a well-conceived set of safeguards that are customized to your organization's specific needs, you can increase the security of your system significantly.

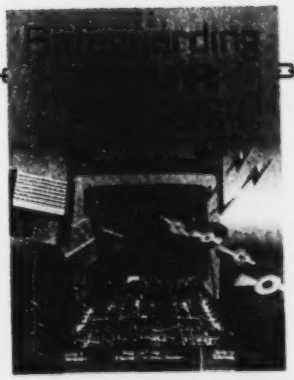
Introductory Security Checklist

While it may be tempting to simply refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement security policy throughout an organization. Other chapters in this document also address ways to customize policy to meet an organization's specific needs—a concept that should not be ignored if you want to ensure the effectiveness of any given guideline.

Security Checklist for Chapter 1

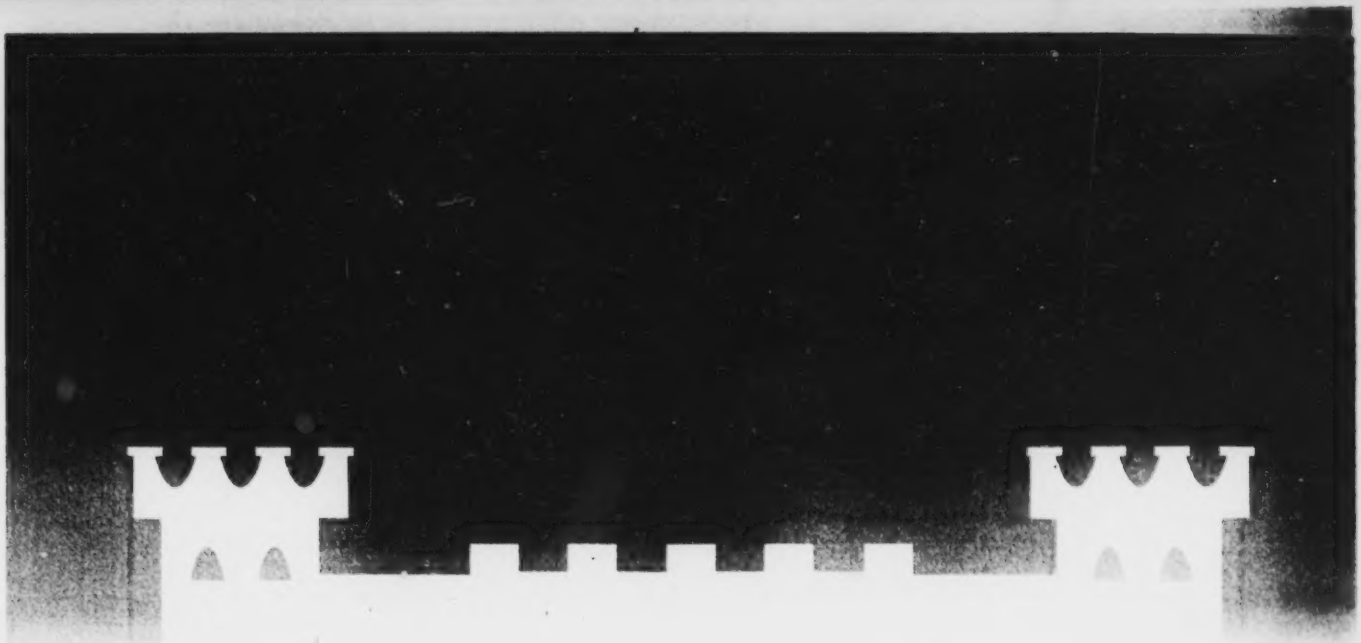
The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points	Page
		1) Are top decision-makers aware that any and all information that is essential to the delivery of educational services should be maintained in a secure manner?	3
		2) Have staff considered the implications of local, state, and federal laws and regulations which require that certain types of education information (particularly individual-level records) be protected from improper release?	3
		3) Has security been made a priority in the organization, as evidenced by top-level staff commitment to read this document and refer to these guidelines while planning the security of the organization's information system?	8
		4) Has a single, empowered staff person (of significant rank) been appointed to manage the organization's security operation?	8
		5) Does the appointed security manager have the appropriate authority and requisite time to do the job properly?	8
		6) Are decision-makers prepared to invest necessary resources in staff security training?	8
		7) Are all employees expected to participate in security initiatives at all times as is applicable (and, secondarily, are they aware of this expectation)?	8



About The Cover Design...

A medieval castle is an integral part of our cover design. Whenever a neighboring Prince Charming turned ugly, these stone and brick edifices were expected to protect the borders, as well as the local populace and their possessions. In today's technological age, security is just as important as it was in the medieval age. Verily, we may no longer be seeking shelter for our pigs and casks of ale, but we are looking for castle-like protection for our sensitive information, files, and equipment.



CHAPTER 2

Assessing Your Needs

CHAPTER 2 IN A NUTSHELL:

Introduction to Risk Assessment	pg 11
Commonly Asked Questions	pg 13
Components of Risk	pg 14
Assets	pg 14
Threats	pg 15
Vulnerabilities	pg 16
Countermeasures	pg 16
Dealing with Risk	pg 17
Guidelines for Risk Assessment	pg 17
The Players: It's a Team Effort	pg 18
Timing: First Things First	pg 19
Take Stock in What You Have and What It's Worth	pg 19
Identify Your Potential Threats and Vulnerabilities	pg 20
Think Through Your Defensive Options	pg 22
Make Informed Decisions	pg 23
Closing Thoughts on Risk Assessment	pg 24
Risk Assessment Checklist	pg 24

Introduction to Risk Assessment

What would the damage be to an educational institution if confidential student aptitude **information** for which it was responsible was lost or misplaced? Would it cost the organization $2,000 to rekey the information? $20,000 to readminister the tests? Perhaps $200,000 in settling legal suits? How about $2,000,000 in technology funding from wary lawmakers who become fearful of entrusting private information about their constituents' children to presumably unsafe record **systems**? Estimating the actual dollar figure for every school building, campus, district, and state education agency is well beyond the scope of a single document—but it is not outside the realm of issues responsible administrators should be considering in their own organizations. After all, if the public and its representative governing bodies were to lose confidence in an education organization's ability to protect **confidential information**, even the most severe estimates of the consequences might not be all that implausible—and a $2,000,000 issue deserves attention.

It can be a risky world out there—a single mistake can get a principal sued, a school board to forbid the exchange of vital education records, or the local legislature to deny technology funding.

So, what could cause a multimillion dollar information leak? An intruder, a negligent operator, or a disgruntled employee? How about a technological snafu? Or even a tornado? A tornado, you ask? It's possible. If those ominous winds were to blow in while your guidance staff was reviewing printed copies of confidential **files,** you could never be quite sure where those records might end up.

How can such a catastrophe be prevented? In the case of a tornado, it probably can't. But like other potential troubles, even the devastating effects of a tornado can be minimized through a well-conceived and properly implemented **security policy.** The first phase in more effectively securing your information and equipment begins with a process referred to as risk assessment. Put simply, risk assessment involves identifying:

- ***Assets*** your organization possesses
- Potential ***threats*** to those assets
- Points in your organization where you may have ***vulnerabilities*** to those threats
- *Probabilities* of threats striking an organizational vulnerability
- *Cost estimates* of losses should a potential threat be realized

Performing a risk assessment is a lot like the early stages of buying insurance—you shouldn't spend your money on protection unless you know exactly what your needs are.

Such an endeavor may seem complicated on the surface, but it doesn't have to be. Risk assessment is a straight-forward process and a most necessary step in decision-making. By evaluating **risk,** you are determining your needs so that you don't spend valuable resources on unnecessary safeguards while, at the same time, you don't leave yourself exposed to unprotected loss.

Risk assessment forces an organization to consider the range of potential threats and vulnerabilities it faces.

What will your risk assessment tell you? Well, since risk assessment is a process and not a product, it depends on your specific situation. As stated above, it should identify your organization's assets, threats, vulnerabilities, probabilities of incursion, and associated costs. How can that help you plan security? It tells you what you have, what it's worth, what to worry about, where you're weak, and why you should be concerned in the first place.

Say, for example, that you realize that the old building in which you store your staff records (an *asset*) was not constructed with fire-resistant materials in the way you would require for a newly built structure (a *vulnerability*)—and you also realize that it's conceivable that a fire (a *threat*) could strike the site (a *probability* that, while low, is real, and could therefore be *estimated)*. The question becomes whether you should introduce **countermeasures** to protect your staff records from a fire.

Knowing what you do about the asset, vulnerability, threat, and probability, the answer then depends upon the cost of replacing that lost asset. If you are in a very small school, it might be feasible to resurvey your staff to gather lost information at relatively little cost; therefore you could afford to risk the loss of staff records.

In contrast, however, while it might also be possible to resurvey staff in a large state system as well, the associated costs would be much greater—so much so that despite the low probability of a fire damaging your *asset* (the records), you wouldn't want to accept the risk because it would be far too costly to assume should the *threat* (the fire) actually strike. Thus, a

small school could theoretically accept the threat of a fire while a large state system should rebuild to meet fire-resistant standards. Right? Not so fast—that's not quite the answer.

While it may seem like a valid conclusion given the information presented, other issues must also be considered. One influencing factor might be that the building in question stores not only staff records, but also student and fiscal records as well, all of which are maintained on a state-of-the-art **computer** system. Suddenly the low cost of resurveying a few teachers doesn't seem like an adequate solution because of the other costs you would likely incur should a fire occur at your site.

Serious discussions of security issues include terms like threats, vulnerabilities, penetrations, and countermeasures because of their precise meanings. While such terminology may seem somewhat out of place in an education publication, it's included in this document all the same in an effort to be consistent with accepted security conventions.

Yet another consideration when evaluating the merit of protection plans is the option of alternative solutions. Yes, rebuilding would be an effective way of protecting your records in the example above, but so might be installing a sprinkler system or training staff to use fire extinguishers. There is also the option of keeping multiple copies of the information in different locations (known in the technical world as "**off-site** backups"). That way, the only chance you have of losing your information would be if there was a combination of highly improbable fires that destroyed both the primary site and each **backup** site. Supplement this with an insurance policy to replace your equipment, and you have yet another effective but less expensive security alternative to rebuilding.

Such an analysis of alternative countermeasures illustrates the importance of working from exhaustive lists of assets, threats, and vulnerabilities.

It is precisely these types of thoughts that the risk-assessment process should elicit. In fact, a properly executed risk assessment provides decision-makers with a methodical approach to determining security strategies—not based on a sales pitch or gut instinct, but on the concrete, context-specific findings of cost/benefit analysis.

In a world of limited budgets, risk assessment provides an organization with the information it requires to accurately prioritize its needs. Options for meeting those needs can then be considered, ranked accordingly, and funded to reflect priority.

Commonly Asked Questions

Q. ***Where do I begin to protect information and equipment?***

A. The answer to that question can be very straightforward if you know the answers to two related questions: (1) What information and equipment do you want to protect? and (2) What do you want to protect it from? Drawing conclusions about these important issues can be accomplished most effectively by a systematic approach to determining your assets, threats, and vulnerabilities—a process referred to here as risk assessment. Risk assessment is a collaborative effort to identify potential threats to your organization's assets, estimate the likelihood of those

threats being realized, and quantify the costs attributable to potential losses.

Q. *Why should I worry about all these details when I have far-reaching insurance policies to cover my losses?*

A. First of all, many insurance policies cover only tangible assets (e.g., equipment). As is emphasized throughout this document, however, information is often more valuable than the equipment that is used to **access** it. After performing a risk assessment, you will be in a better position to inquire about additional insurance policies to cover your information as well. You can then make sure that you have insured yourself against reasonably probable, high-cost losses because risk assessment will have helped you determine what they are more likely to be. Remember, as an educational administrator, you are the expert on your organization, not an insurance agent. It is your job to know where and why you need insurance coverage—so review all policies after performing your risk assessment. Don't pay for insurance you don't need and make sure that you have those policies you do need.

Q. *Even if my risk assessment identifies real threats and vulnerabilities, how can I possibly deal with them with such a small staff (not to mention budget)?*

A. The fewer the **resources** you have to put into protecting your organization, the more vital the risk assessment process becomes. Think about it. If you have unlimited security funding, then you may have enough resources to protect yourself against the entire spectrum of threats. Having said that, however, it should be noted that even the wealthiest organizations should perform a risk assessment to be sure that they have considered all of their potential threats. On the other hand, if funds are scarce, you need to perform a risk assessment to accurately prioritize your needs before allotting your limited resources. In this way, risk assessment provides you with the information needed to address your most pressing needs first and increase the effectiveness of those resources that are at your disposal, whatever they may be.

Components of Risk

What is a risk? For the purpose of information security and this document, a risk is any hazard or danger to which your information or equipment is subject. Storing an expensive computer within reach of an open window is risky. Allowing students to have access to **computerized** grade books might also be considered risky. But even if you now know what a risk is, the question of what is at risk still remains—and the answer is your assets.

Assets

An asset is often defined as real property. This being the case, it's quite probable that your organization's computer equipment is prominently listed on the balance sheets as an asset—a fitting designation, especially considering the large amounts of money that the equipment surely cost. But recall that the only reason all those dollars were spent on technology in the first place was so that you could manipulate your organization's information more efficiently—information like student academic **data,**

special support service files, staff health records, and organizational financial figures. The equipment is important only because it is the mechanism by which you access the files that are so essential to the operation of the educational enterprise. Information is the real asset.

Equipment is, of course, very valuable, but never forget that the real asset is the information.

Threats

It is estimated that as much as 67 percent of **networked** computers are infected with one form of a **virus** or another in a given year.[3] Even accounting for the growing prevalence of virus threats, more than half of all reported system damage is caused by unintentional employee action—in most cases, simple negligence. Any such action, actor, or event that contributes to risk is referred to as a threat.

Examples of Threats to an Organization's Assets

Natural Threats

Lightning	Tornado	Hurricane
Flood	Earthquake	Snow/Ice Storm
Forest Fire	Humidity	High Temperatures
Dirt	Rain/Water Damage	Time (Aging Media)

Manmade Threats (Intentional)

Theft	Vandalism	Arson
Hacking	File Sabotage	Wire Taps
Computer Viruses	Unauthorized Copying	

Manmade Threats (Unintentional)

Equipment Failure	Power Fluctuations	Magnetic Fields
Spilled Beverages	**User** Error	Air Conditioning Ducts
Computer Viruses	Heating Units	**Programmer** Error
Lost Documentation	Lost **Encryption Keys**	Aging Facilities

Although there appears to be more threats that come from outside of the organization, internal threats (e.g., authorized users who are either accident-prone, negligent, or criminal) are far more likely to breach system security than external threats.

As you consider types of potential threats, notice the secondary distinction that becomes relevant in the manmade category between intentional and unintentional threats. Intentional manmade threats are a source of particular resentment for many people. After all, why should an organization have to spend its valuable resources on keeping users from willfully causing damage? The same question can be asked about the need for uninsured motorist insurance, but the results will be the same. You have to be able to account for people who are unwilling to play by the rules!

Deliberate unauthorized assaults on a system can make sense to potential intruders when two conditions are met:[4]

1) The intruder can benefit substantially from the act (i.e., something of value can be gained).
2) The act requires relatively little effort in comparison with the potential gains.

The message is clear:

Know the potential value of your information and make penetration more difficult than it's worth.

Threats and vulnerabilities exist whether you are aware of them or not—risk assessment helps to inform decision-makers of their presence.

Vulnerabilities

Vulnerabilities refer to points within a system that are open to **attack** or damage. What type of attack? That depends on the threat. Vulnerabilities are the mechanisms by which threats access your system. Think of a thief (a threat), for example, who is ready to strike your building (which houses your assets). An open back window through which that thief might enter the premises is a *vulnerability*.

Countermeasures

A countermeasure is a step planned and taken in opposition to another act or potential act. While ultimately aimed at rebuffing threats, countermeasures are often deployed strategically at points of vulnerability, as is the case when a lock (a countermeasure) is installed on a back window through which a thief may try to enter your building (see vulnerabilities above). Countermeasures are often designed to serve one of the following functions:[5]

- **Prevention** — For example, by initiating backup procedures, threats are prevented from damaging your lone copy of information in a single event.
- **Deterrence** — For example, by training users about the legal consequences of unacceptable use, potential threats who might otherwise consider destructive activities may be deterred.
- **Containment** — For example, by segmenting each separate type of information in your system, even active threats can be limited to the record areas they can find and enter.
- **Detection** — For example, by reviewing records of user activity, commonly referred to as **audit trails,** unwelcome activity can be uncovered.
- **Recovery** — For example, by preparing and testing a **contingency plan,** "lost" systems and "damaged" information can be salvaged (or at least losses and damage can be minimized).

Dealing with Risk

Creating a risk-free environment is unrealistic, but instituting a "**trusted system**" (i.e., one that while not perfect is trustworthy) is possible.[6] The reason for this limitation is that you simply cannot counter all risk. In actuality, countering risk is only one of three potential ways in which to deal with threats and vulnerabilities. Although it may seem counter-intuitive based on the stated purpose of this document, risk can also be accepted (sometimes a very stable strategy) or ignored (not a good plan under any circumstances).

Options for dealing with risk:
(1) *Counter* it (an informed decision)
(2) *Accept* it (also an informed decision)
(3) *Ignore* it (an uninformed decision and a poor strategy)

Under what conditions could accepting risk make sense? Well, it is theoretically possible that an asteroid could smash into the earth and land, of all places, on your office. The risk is real, albeit small, and can be estimated as such. Should you, therefore, endeavor to build a concrete vault two miles beneath the surface of the earth to store backup files of your records, or should you accept the risk of an asteroid strike and figure that your system will be the last of your worries should the event actually occur? Your risk assessment (see Steps 1-8 below) and common sense will probably tell you that you can safely afford to accept the residual risk of asteroid strikes. That's right, you don't have to counter any and every risk conceivable, only those it makes sense to address based on the results of your risk assessment.

On the other hand, ignoring risk is not a stable strategy (although it is an all too common practice). Risks are everywhere. If you choose not to perform a risk assessment and, instead, simply choose to ignore your risks, they are still there all the same—you just won't be prepared for them. Thus, despite the fact that it is possible to handle risk in any of the three ways—counter it, accept it, or ignore it—only the first two are stable strategies, and both depend on the results of an accurate risk assessment.

While potential risks should never be ignored, it only makes sense for an organization to focus its attention on those risks that are most likely to affect the system.

Guidelines for Risk Assessment

A properly conceived and implemented risk assessment should:[7]

- Provide the basis for deciding whether countermeasures are needed
- Ensure that additional countermeasures counter actual risk
- Save money that might have been wasted on unnecessary countermeasures
- Determine whether residual risk (that risk which remains after countermeasures have been introduced) is acceptable

You don't want to put a 50-dollar lock on a 20-dollar hammer—unless you're a carpenter and you would lose more than 50-dollars' worth of business in the time it took to replace that 20-dollar tool.

Risk Assessment Outline

The Players: It's a Team Effort

Timing: First Things First

Take Stock in What You Have and What It's Worth

- Step 1 - Identify Sensitive Information and Critical Systems
- Step 2 - Estimate the Value of System Components

Identify Your Potential Threats and Vulnerabilities

- Step 3 - Identify Threats
- Step 4 - Identify Vulnerabilities
- Step 5 - Estimate the Likelihood of a Potential Penetration Becoming an Actual Penetration

Think Through Your Defensive Options

- Step 6 - Identify Countermeasures Against Perceived Threats and Vulnerabilities
- Step 7 - Estimate Costs of Implementing Countermeasures

Make Informed Decisions

- Step 8 - Select Suitable Countermeasures for Implementation

If top educational administrators in an organization don't actively participate in, and outwardly demonstrate their commitment to, the security effort, no one else in the organization will either.

The Players: It's a Team Effort

The process of risk assessment should be initiated and led by the top educational administrators in an organization. But although the endeavor is captained by chief administrators, feedback from all levels and job categories is required. At a minimum, information collectors, data providers, data entry staff, and data processors and managers should be involved in the early stages of risk assessment. In short, more people involved in the brainstorming process results in more ideas being generated.

It Really Happens!

A large and technologically sophisticated school district was having difficulties with the good practice of backing up its networked computer files each night. It seemed that despite the data manager's best efforts to verify that all of the computer equipment used in the copying process was working properly, one portion or another of the tapes would invariably fail to copy every night—namely, there would always be a "blank spot" on the backup file where nothing had actually been copied. To make matters more perplexing, the data manager, well-trained in her field, had finally decided to try running the backup procedures in the middle of the work day just to test the equipment. Surprisingly, after repeated failures in the evenings, the process worked perfectly. Now thoroughly frustrated by the situation, she decided to stay several hours after work so that she could observe the backup system in action first hand. Three hours after everyone but the cleaning staff had left for the day, the tapes began the automatic copying process without a hitch. The data manager monitored the tape speed, the cabling between the computers, and even the room temperature. In fact, she was so totally engrossed with her inspection of the system that she barely noticed the custodian when he walked into the room and said hello. The focused woman, somewhat startled by the man, looked up to reply to the greeting—only to see him pulling the backup computer's power cord from the outlet in order to plug in his vacuum cleaner. "So," she said to herself ironically, "that's why we have such a clean computer room."

Timing: First Things First

Risk Assessment is a prerequisite for any serious attempt to implement a security policy within an organization. It's a step that simply cannot be ignored. After all, unless the organization's needs are first accurately assessed, there is no way of knowing whether financial and staff resources are being wisely invested in security initiatives.

While it is never too late to do the right thing, postponing risk assessment invites undue peril and unnecessary liability.

Take Stock of What You Have and What It's Worth

Only careful and collaborative efforts will yield worthwhile results. Be inclusive, exhaustive, and realistic when documenting your assets.

▶ **Step 1 - Identify sensitive information and critical systems:** The goal here is to make a distinction between **general information** and **systems** (i.e., that information and those systems that are helpful to your organization as it carries out its mission) and **sensitive information** and **critical systems** (i.e., that information and those systems that are private and/or vital to your organization as it carries out its mission).

For example, the computer that houses the "HELP" file for your organization's word processing **software** is a "general" support component. While it is most helpful to have access to user HELP when facing a word processing problem, the files themselves are not vital to running a school or school system. Conversely, the new software that manages a school system's substitute teacher scheduling is vital to the teaching mission. If it isn't available and working properly, principals could potentially find themselves with classrooms full of students who have no teacher. And that makes the system "critical" if ever there was one.

Sensitive information **is that information which if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.**

▶ **An example of sensitive information would be personal student or staff records.**

Critical systems **are those systems or system components (hardware or software) that if lost or compromised would jeopardize the ability of the system to continue processing.**

▶ **An example of a critical system might be the cabling that links your administrative and instructional computer networks.**

Don't allow yourself to feel restricted when brainstorming—among other pitfalls, avoid working within the paradigm of conventional technical definitions if you feel that they might limit your ability to construct an exhaustive list of your assets. For instance, when considering critical systems, don't restrict yourself to physical systems, which traditionally require actual **hardware** connections. In your organization and information system, perhaps two stand-alone computers in the same room constitute a single system. Remember, the primary consequence of Step 1 is that all equipment and information identified as being either sensitive or critical needs to be given strong consideration as high priorities on the list of concerns that demand security. To leave out a component because you didn't think broadly enough leaves the organization vulnerable.

▶ **Step 2 - Estimate the value of system components:** Estimating the value of your information system is not always simple, but the task is made more manageable by focusing on the word "estimate." After all, it

It must be acknowledged that while even a well-reasoned estimate is little more than an educated guess, it is still a better gauge of reality than wild speculation or, even worse, blatant disregard.

may very well be impossible, or at least impractical, to try to derive a precise dollar value for some assets (especially information assets). Instead, try to calculate a reasonable approximation of the replacement value of each component of the system—both equipment and information. Be sure to consider the following factors when deriving your estimation:

- Direct replacement costs of hardware, software, and **peripherals** (Would there be installation costs? Consultant fees? Necessary **upgrades**?)
- Replacement costs of stored information (Would rekeying be necessary? Resurveying?)
- Costs associated with the disruption of service or other activities (Would you have to pay staff overtime during the recovery period? What about extra school days at the end of the year to make up for missed time?)
- Indirect but real costs associated with a loss of public confidence (Would it impede current or future data collection efforts? What would be the effect on legislative initiatives?)

Again, keep in mind that while the costs of hardware and software tend to be more readily measurable, information costs are very real as well. You may not be able to call a vendor and say "What is my information worth?" the way you can call your equipment salesperson, but you still have to ask yourself "What is it worth to my organization?" Estimates of these costs, no matter how rough, give you a more accurate sense of the true value of important information assets.

Remember that people often rely on information in their school records for their entire lives—to get jobs, to apply to schools, and to verify age and credentials. Dollars and cents may be a poor measure of the value of such information.

One common mistake in this process that can lead to serious flaws in assessment results is when you focus on only the sensitive and critical segments (as identified in Step 1) when estimating the value of an information system. While identifying sensitive information and critical systems is necessary for setting priorities, all information has value and requires attention in this step. If it doesn't, the information's overall utility should be reconsidered. After all, if it isn't valuable enough to recover or rekey upon being damaged (which requires a cost that can be estimated), what purpose could it possibly be serving?

If information isn't valuable enough to warrant consideration of its protection and recovery, can it be valuable enough to warrant precious disk space in the first place?

Identify Your Potential Threats and Vulnerabilities

How do you identify threats and vulnerabilities? In a word: Brainstorm! No idea about potential threats or vulnerabilities is unimportant. However, keep in mind that management has a very limited perspective on information and system use. Maximize the resources at your disposal by including representatives from all organizational levels and duty types in the brainstorming effort. After all, you don't want that

cleaning staff left out when they might be the only people on duty to protect equipment and information after hours. Nor do you want to exclude those library assistants who oversee the computers your students use to **log on** to the **Internet.** Always keep an open mind to what your users have to say.

▶ **Step 3 - Identify threats:** What actors, actions, or events threaten your system? Refer to the examples on page 15 before creating an exhaustive list through a collaborative brainstorming process. Be sure to consider the following types of threats:

- Natural (e.g., fire, flood, lightning, and humidity)
- Manmade unintentional (e.g., negligence and accidents)
- Manmade intentional (e.g., **hackers** and viruses)

▶ **Step 4 - Identify vulnerabilities:** Where is your system susceptible? Consider vulnerabilities to natural threats and both intentional and unintentional manmade threats as identified in Step 3. Also look at other examples of threats, as listed on page 15, to see if any new ideas are triggered. After this initial brainstorming, organize the list of vulnerabilities you've generated into categories such as the following and then once again see if additional thoughts come to mind:

- Physical concerns (e.g., room access, building construction, and climate)
- Hardware- and software-related issues (e.g., equipment, **programs,** and compatibility)
- Media liabilities (e.g., **disks, tapes, hard drives,** and print copies)
- Communications (e.g., access points and **encryption**)
- Human concerns (e.g., personnel and office behavior)

Where Is Your Office Vulnerable?

The following happens in the typical office quite frequently:

- A door is propped open and doesn't have a lock (see Chapter 5).
- A cup of coffee is set on a computer case (see Chapter 5).
- A computer monitor sits within plain sight and easy reach of a window (see Chapter 5).
- Wiring is in the way of foot traffic (see Chapter 5).
- Equipment is plugged into wall sockets without a surge protector (see Chapter 5).
- Outlets are overloaded (see Chapter 5).
- Backup files are stored in the same room as the original files (see Chapter 6).
- Floppy disks are shared haphazardly and are not labeled (see Chapter 6).
- Someone's password is written and posted on their monitor (see Chapter 8).
- A computer is logged on but has been left unattended (see Chapter 8).

Is any of this happening in your office?
If it is, your system is vulnerable!

▶ **Step 5 - Estimate the likelihood of a potential penetration becoming an actual penetration:** What is the probability of a threat capitalizing on a vulnerability? As difficult as answering such a question might appear to be, you don't have to be able to predict the future in order to generate reasonable probabilities of future events. Use logic, as possible, to support your estimates. For example, for an institution located along the Mississippi River, earthquakes and floods are threats that are within the realm of possibility, but logic will tell you that the site is probably much more susceptible to floods. Using flood histories, the likelihood of the next 100-year flood can be estimated. Similarly, by researching earthquake data, you can estimate the likelihood of earthquakes as well.

Think Through Your Defensive Options

▶ **Step 6 - Identify countermeasures against perceived threats and vulnerabilities:** This step parallels Steps 3 and 4 in that its purpose is to generate an exhaustive list of ideas—this time potential solutions to the concerns caused by your identified threats and vulnerabilities. When considering options, be sure to keep in mind that many threats and vulnerabilities can be addressed by more than one countermeasure. A potential thief, for example, could be thwarted by better locks, video cameras and other electronic surveillance, or even trained security patrol officers. Step 6 focuses on generating a list of such options for each perceived threat and vulnerability, *not* in selecting what appears to be the preferred option. That is attempted only after an exhaustive list is finalized and costs/benefits are considered. Issues to consider when brainstorming potential countermeasures include:

For recommended countermeasure options, see Chapter 5 (Physical Security), Chapter 6 (Information Security), Chapter 7 (Software Security), Chapter 8 (User Security), and Chapter 9 (Network Security).

- Physical security equipment and procedures—location and environmental strategies such as climate monitors, required building specifications, and regulations governing room access and food and beverage use
- Information security practices—storage and use regulations such as **labeling** and **write-protecting** files
- Software security techniques—purchasing and programming concerns such as copyright infringements and proper documentation
- User access controls—data and system access issues, including log-in and password protection
- Networking security initiatives—connectivity issues like **firewalls** and encryption strategies

A big screen television is nice, but not if it's in a room that is 8 feet wide by 9 feet long. So, too, must countermeasure solutions be compatible with an organization's environment in order to be effective.

Estimates should account for both start-up and maintenance costs.

▶ **Step 7 - Estimate costs of implementing countermeasures:** This step entails determining the costs associated with countermeasures identified in Step 6. Remember that the vast majority of costs are twofold: initial and ongoing. Be certain to consider all of the following factors:

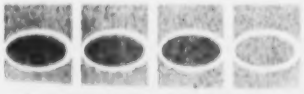
- Both money and time for research, development, procurement, installation, and maintenance of security features
- Staff training time—the costs are real and absolutely necessary

- It Really Happens!

The local elementary school decided to purchase five new computers for its media center—no small investment considering its limited technology budget. Mr. Watkins, the librarian, would supervise their use and was in charge of the acquisition. He went down to the computer store to inspect the merchandise one last time before making a final commitment. While he was there, he bumped into the salesperson who had so ably advised him throughout the selection process. As they chatted, Mr. Watkins mentioned that he was very excited about the purchase, but also a bit nervous. "I've never had to run a computer lab before," he admitted. "In truth, I bet that the students know more about these computers than I do." The salesperson, with the best of intentions, mentioned that the store offered a service package that provided on-site maintenance on equipment they sold for only $100 per piece per year. Mr. Watkins immediately agreed to order the package, deciding that it was a waste to spend all that money on the equipment in the first place if he was not properly trained to keep the machines up-and-running. Privately, he absolutely dreaded the thought of having kids running throughout the lab with nothing to do as he tried to tinker with the complicated equipment in vain.

Two months later, after the new computers had been purchased and installed, Mr. Watkins noticed that one of the monitors wouldn't turn on properly. Not wanting to push a panic button, he called the building custodian to check the outlet. "Nah, it's not the power," the custodian reported. "We'd better get the guys from central office down here." Mr. Watkins looked at him with surprise, "Why would we bother them when I have a service contract from the store where I bought the monitor?" At that point, two months after an extra $500 had been spent on maintenance contracts, Mr. Watkins finally found out that the school district serviced instructional equipment at no cost to the schools. "Wow," he thought as he looked with despair at the service contract he had purchased without much consideration, "what a waste of money!"

- Altered productivity (e.g., having each employee spend one minute using a **virus scanner** three times each day may amount to only three minutes of work time per day, but when calculated for the entire organization and compounded by a host of other possible security activities, such seemingly insignificant costs can add up)
- Countermeasures already available to the organization that may require less investment to institute (e.g., if your accounting office currently uses certain security procedures, there may be fewer training costs because you already have a core of people who can share their expertise)



Recognize that because of the gray areas associated with estimating the value of information and the likelihood of threat incidents, risk assessment is not an exact science—don't be afraid to leave yourself some room to adjust your findings so that you can accommodate good, old-fashioned common sense.

Make Informed Decisions

▶ **Step 8 - Select suitable countermeasures for implementation:** In Step 8, it's finally time to decide which countermeasures make the most sense to implement. Remember that there will probably be more than one countermeasure that can protect your system from any given threat or vulnerability, so you have some choices. Your job is to determine which strategy makes the most sense from a cost/benefit perspective. This can be accomplished by comparing your estimated costs of potential losses for a given period of time (Steps 2-5) with actual security costs that would be incurred when preventing such a loss for the same period of time (Step 7).

A desired level of risk reduction is achieved when further reduction would cost more than the benefits gained.

One way to decrease your actual security costs is to keep in mind that a single countermeasure can actually serve as a solution to multiple threats and vulnerabilities. An example of this is when security officers who protect your most sensitive areas serve as a countermeasure to both external intruders and potentially misguided staff. Such a compromise solution is really no compromise at all—two potential threats are being countered for the price of one. In effect, you're getting twice the protection for the cost of a single countermeasure!

Closing Thoughts on Risk Assessment

Once you determine your needs and priorities through the above eight steps, you can then make security decisions based on concrete information. Sales pitches from vendors and gut instinct on the part of well-intentioned, but perhaps uninformed, staff need no longer serve as reasons for making security policy when competent administrators are armed with the information required to make rational, valid decisions.

It should be emphasized that decision-makers must be involved in the entire process of risk assessment. Should, instead, they rely simply upon cost/benefit analysis without being aware of other important factors that might have been uncovered in the process, they might not make a completely informed decision. A good example of this would be if it was determined in Step 1 that some of the student information on a computer was actually sensitive. As discussed throughout this document, those confidential records would need to be protected regardless of cost/benefit analysis because of the various laws in place that mandate protection of student and family education records. Not knowing this important fact could, in such an instance, lead to disastrous results for the organization and its students!

An exception to the rule: Failure to introduce risk reduction cannot be justified by cost/benefit analysis if there are compelling non-financial reasons for mandating it (e.g., privacy or appropriate use laws).

Risk Assessment Checklist

While it may be tempting to simply refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement security policy throughout an organization. Other chapters in this document also address ways to customize policy to meet an organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 2

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points for Risk Assessment	Page
		1) Is the process of risk assessment being championed by a top-level decision-maker?	18
		2) Is feedback being elicited from representatives of all user types?	18
		3) Have sensitive information and critical systems been identified (Step 1)?	19
		4) Has the value of all system components (not just sensitive information and critical systems) been estimated (Step 2)?	19
		5) Has an exhaustive list of potential threats been generated (Step 3)?	21
		6) Has an exhaustive list of vulnerabilities been generated (Step 4)?	21
		7) Has the likelihood of a potential penetration becoming an actual penetration been estimated (Step 5)?	22
		8) Has an exhaustive list of countermeasures to identified threats and vulnerabilities been generated (Step 6)?	22
		9) Have the costs of implementing identified countermeasures been estimated (Step 7)?	22
		10) Have suitable countermeasures been selected for implementation (Step 8)?	23

An ounce of prevention is worth a pound of cure. —Unknown

CHAPTER 3

Security Policy: Development and Implementation

CHAPTER 3 IN A NUTSHELL:

Why Do You Need a Security Policy? pg 28
Commonly Asked Questions pg 28
How to Develop Policy pg 29
- Getting Perspective pg 29
- What to Include pg 30
- Writing with Proper Tone pg 30
- From the Board Room to the Break Room: Implementing Security Policy pg 31
- Personnel Issues pg 33
- A Special Note on Outsiders pg 33

Closing Thoughts on Policy pg 34
Policy Development and Implementation Checklist pg 34

It Really Happens!

Like many people, Fred Jones thought he had a difficult job. As the Information Systems Manager in a small school district, he was responsible for operating a district-wide computer network—everything from installation and maintenance to user support and training. While it was clearly not a one-man job, he was his own one-man staff. Fred had tried to explain to his superintendent that the district's network was vulnerable to a range of threats because his small budget and non-existent staff prevented him from handling system security effectively, but his warnings had always been ignored

One morning at a staff meeting, and much to Fred's surprise, the superintendent announced that he had read a newspaper article about a student breaking into a neighboring school district's computer system and changing report card records. The boss proceeded to declare that Fred was now being charged with developing and instituting a computer security policy for the school district.

As soon as the meeting was over, Fred approached the superintendent to request an appointment for them to discuss a shared vision for development of the security policy. "Effective security policy requires input and commitment from the whole organization, so I think we should sit down and map out a plan for developing our security policy," Fred asserted.

But the superintendent declined the invitation to participate in the policy-development process. "Fred, I'm just too busy to get involved in this project. I trust you to do a job that will make us all proud." When Fred asked about expanding his staff and budget to meet the increased workload, the superintendent again dismissed the issue. "Fred, times are tough and the budget is lean. Maybe next year we'll be able to work something out. In the meantime, you get cracking on securing our system as if your job depends on it... in fact, I guess your job does depend on it."

Fred watched his unrealistic, if well-intentioned, boss walk away, realizing that his job was no longer difficult, but truly impossible. He was now expected to develop, institute, manage, and monitor an organization-wide security policy without assistance, consent, or buy-in from a single employee, much less empowered high-level administrators. He knew that the organizational support he failed to receive meant that there was little chance of his being able to effectively secure the system—and that it was just a matter of time before a significant breach in system security would take place. Fred found himself in the terrible position of being responsible for stopping the inevitable, yet powerless to do so.

Why Do You Need a Security Policy?

While the organization is responsible for securing confidential information, should there be a breach, it is the chief administrator who sits in the "hot" seat.

Who is responsible for securing an organization's **information**? Perhaps the Research and Evaluation department? Not exactly. The Management Information System (MIS) staff? Wrong again. Ultimately, it is not only individual employees or departments that are responsible for the security of **confidential information,** but also the institution itself. It is, therefore, incumbent upon top administrators, who are charged with protecting the institution's best interests, to ensure that an appropriate and effective **security policy** is developed and put into practice throughout the organization.

While policies themselves don't solve problems, and in fact can actually complicate things unless they are clearly written and observed, policy does define the ideal toward which all organizational efforts should point. By definition, security policy refers to *clear, comprehensive,* and *well-defined* plans, rules, and practices that regulate **access** to an organization's system and the information included in it. Good policy protects not only information and **systems,** but also individual employees and the organization as a whole. It also serves as a prominent statement to the outside world about the organization's commitment to security.

Commonly Asked Questions

Q. ***What does this document have to offer that experienced education policy-makers don't already know?***

A. Experienced policy-makers certainly bring a great deal of skill to security policy development. But in many ways, security policy is different from other forms of more traditional policy—it requires policy-makers to think like **data** entry clerks, MIS staff, research and evaluation specialists, legal counsel, building administrators, teachers, and so on. Many of the procedural guidelines included here will already be appreciated by seasoned policy-makers, but this document tailors the information so that it can be more readily applied to the specific concerns of information and system security—an area of expertise not always held by educational administrators and policy-makers.

Q. ***Isn't policy written at the district and state level?***

A. Yes, but not exclusively. Whoever is in charge of a site (be it a building, campus, district, or state education agency) must be concerned about protecting **sensitive information** and **critical systems** that can be accessed from within that site. This concern is articulated through security

policies that are designed to regulate access and protect information and systems as circumstances within the organization specifically warrant.

Q. ***Shouldn't expert technology consultants be hired to do the job?***

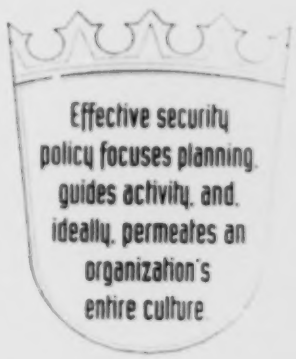
A. There certainly are roles for expert consultants when instituting security policy: they could be hired as general technical support or they might be useful in offering advice about **countermeasures** (e.g., a **password** system). But generally speaking, the chief educational administrator and his or her employees need to shoulder the responsibility of protecting their system because, after all, it is their system. They are the people who know it best and they will be the ones who have to implement adopted security policy. Outside contractors, while certainly capable of lending expertise to the process, cannot take the place of committed and informed staff.

How to Develop Policy

Tenable security policy must be based on the results of a **risk assessment** as described in Chapter 2. Findings from a risk assessment provide policy-makers with an accurate picture of the security needs specific to their organization. This information is imperative because proper policy development requires decision-makers to:

- Identify sensitive information and critical systems
- Incorporate local, state, and federal laws, as well as relevant **ethical standards**
- Define institutional security goals and objectives
- Set a course for accomplishing those goals and objectives
- Ensure that necessary mechanisms for accomplishing the goals and objectives are in place

In this way, legal and regulatory concerns, organizational characteristics, contractual stipulations, environmental issues, and **user** input can all be incorporated into policy development. Effective security policy synthesizes these and other considerations into a clear set of goals and objectives that direct staff as they perform their required duties.



The Logic of Well-Planned Policy

If: Organizational needs define policy

and: Policy guides personnel and technology decisions

then: Personnel and technology serve organizational needs.

Getting Perspective

Although finalizing organizational policy is usually a task reserved for top-level decision-makers, contributing to the development of policy should be an organization-wide activity. While every employee doesn't necessarily need to attend each security policy planning session, top-level administrators should include representatives from all job levels and types in the

If staff have minimal input in policy development, they may show minimal interest in policy implementation.

information gathering phase (just as in the case of brainstorming during risk assessment). Non-administrative staff have an especially unique perspective to share with policy-makers that simply cannot be acquired by any other means. Meeting with staff on a frequent basis to learn about significant issues that affect their work is a big step toward ensuring that there is buy-in at all levels of the organization.

Reviewing security arrangements in other organizations might uncover information that can contribute to more effective policy development.

While it makes sense to get as much input from potential users as is possible, it is also essential that voices from outside the organization be heard during the information gathering stages of policy development. Why? Because decision-makers need to be informed of security arrangements that other organizations are making that potentially impact them and the policies they will be developing. If, for example, every school but one in a district commits to **encryption software** to protect messages sent over the Internet, the lone school that does not have the encryption **key** is going to have a very difficult time communicating with its partners. The point is that just as security planning demands coordination internally, it often requires it externally as well—a recommendation that should not be overlooked, especially by those organizations that practice site-based management.

Creating consortia, cooperatives, and other types of associations enables organizations to pool resources and share expenses as they endeavor to devise and implement security strategies.

What to Include

An organization's risk assessment, and not this document or any other source, informs policy-makers of their system's specific security needs. But regardless of those findings, the following general questions should be addressed clearly and concisely in any security policy:[9]

- What is the reason for the policy?
- Who developed the policy?
- Who approved the policy?
- Whose authority sustains the policy?
- Which laws or regulations, if any, are the policy based on?
- Who will enforce the policy?
- How will the policy be enforced?
- Whom does the policy affect?
- What information **assets** must be protected?
- What are users actually required to do?
- How should security breaches and violations be reported?
- What is the effective date and expiration date of the policy?

Writing with Proper Tone

Policy should be written in a way that makes sense to its intended audience. After all, guidelines that aren't implemented foreshadow objectives that won't be met. Tips for reader-friendly policy include:[10]

- Be concise—focus on expectations and consequences, but explain the underlying rationale when appropriate
- Don't temper the message—truth is, you're not asking but telling, so don't propose, suggest, or insinuate unless that is specifically what you mean to do
- Use simple, straightforward language as is possible
- Define any term that could potentially confuse a reader—no need to make things more difficult than need be
- Be creative—presentation should never interfere with content, but checklists and reference cards increase utility

Another hint for ensuring appropriate tone is to word policy in a way that makes sense to both developers and users before giving the draft to legal counsel. The purpose for this is to keep clear and meaningful points from being transformed into incomprehensible legal jargon. If the official policy does eventually get transformed into something particularly formal, consider rewriting a distributable version designed specifically for reader-friendliness.

Rewrite formal policy into a reader-friendly version that is distributed to staff.

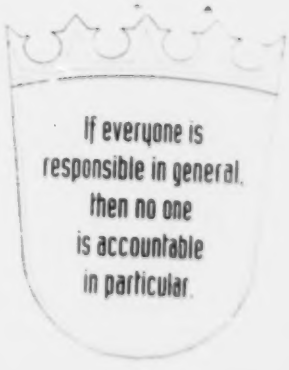
From the Board Room to the Break Room: Implementing Security Policy

This document presents a great deal of information for policy-makers to consider. The role of an effective administrator, however, is to absorb these recommendations as appropriate and distill the results into a meaningful and manageable set of employee regulations that fit his or her organization. These rules then serve as the mechanisms for operationalizing policy goals and objectives throughout the workplace. Although it might be tempting (and certainly possible) to create an exhaustive inventory of "do's and don'ts," formulating a short list of sensible rules that can realistically be implemented is undoubtedly a better strategy.

Read Chapters 5-9 for specific security guidelines to support your policies.

Policies that are neither implementable nor enforceable are useless—ten security regulations that are implemented are more effective than 110 that are ignored.

How can policy implementation be made realistic? Aside from keeping regulations clear, concise, and understandable, endeavor to make them as easy as possible for staff to fulfill. Remember, the goal is not to tell staff "how it is" as much as to get everyone to join in the effort. By keeping things as simple as possible, employee participation becomes a realistic aspiration. Specific actions that increase the likelihood of your policies actually being realized in the work environment include:



- *Specifically assign an empowered and committed administrator to be accountable for security:* Someone must make security a day-to-day priority. This designated staff member must be authorized to both reward and reprimand employees, as necessary, at all levels of organizational hierarchy. (see Chapter 4, Security Management)
- *Institute staff training that is specifically tailored to meet the requirements of security policy and the needs of your staff:* Recognize that most **computer** users have never been trained to properly use technology—and what little training they do have was probably

aimed at overcoming their fears and teaching them how to turn on their machines. At most, they may have learned how to use a particular piece of software for a specific **application**. Thus, the majority of your staff have little understanding of security issues, and there is no reason to expect that to change unless the organization does its part to correct the situation. Reluctance on the part of the organization to adequately prepare staff for making security policy a part of the work environment makes the rest of the effort an exercise in the theoretical—and theory won't protect a system from **threats** that are all too real (see Chapter 10, Training).

Unless the organization educates its users, there is little reason to expect security procedures to be implemented properly.

Increase security awareness by making security references readily available.

- *Communicate organizational needs and expectations to staff in both initial and ongoing ways:* Make a serious attempt at getting the word out to staff, but don't be overly serious in its presentation. Just like in any marketing campaign, creativity and consistency will be rewarded by audience responsiveness. The following examples are recommended as effective strategies for communicating security expectations to staff:
  - Hold security refresher workshops.
  - Create an infrastructure to support staff (e.g., a **Help Desk** that is staffed with competent and readily available advisors).
  - Acknowledge exceptional behavior frequently and publicly.
  - Develop and distribute reference materials (e.g., checklists, brochures, and summaries—remembering that succinct and reader-friendly material is much more useful than an unabridged tome of security obscurities).
  - Update the employee handbook to reflect security procedures.
  - Keep security reminders visible throughout the workplace (e.g., posters, FYI memos, and **e-mail** broadcasts).

Because most people are unwilling to act unless they believe they are personally responsible, each user must be held individually accountable for specific security functions.

- *Enforce security regulations equally at all levels of the organization:* Each individual in the system must understand that he or she is personally accountable for security. Bosses have to say "get with the system," mean it, and prove it by doing so themselves. If the rules don't apply to everyone, then they apply to no one. This is not simply an egalitarian moral—if the system is not secure from top to bottom, then, by definition, it is not secure!

Expecting every employee to become a security expert is wholly unrealistic. Instead, break down recommended security practices into manageable pieces that are tailored to meet individual job duties. A single, short and well-focused message each week will be better received than a monthly volume of information that is overly ambitious.

If your institution has several types of work environments or levels of users, consider writing separate security regulations, all of which support broader policy, for each user group. Each policy can then be tailored to the specific needs of the particular environment or user type. To increase involvement and acceptance, have staff contribute to the development of their own policy guidelines and procedures. For completeness and

consistency across the institution, each user group may require the services of an expert security coordinator while developing its own subset of guidelines.

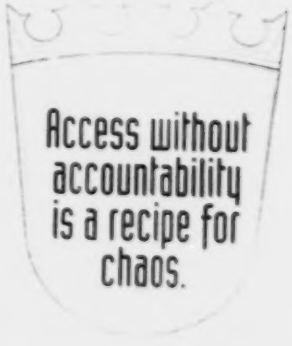
Personnel Issues

One aim of successful security policy is that it should limit the need for trust in the system. While this may seem like a terribly cynical philosophy, it actually serves to protect both the organization's employees and the organization itself. But before the benefits of security can be realized, staff must be properly informed of their roles, responsibilities, and organizational expectations.

- Employees must be told in *writing*:
  - What is and is not acceptable use of equipment.
  - What the penalties for violating regulations will be.
  - That their activities may be monitored.
  - That security will be a part of performance reviews (users who do their share should be rewarded, whereas those who lag behind might be reprimanded or retrained).
- Employees should be reminded that:
  - Organizational **resources,** including computers, belong to the organization.
  - There should be no expectation of privacy for information stored on or transmitted with the organization's equipment.
- Employees should be required to sign a Security Agreement (see Appendix D for a sample) to acknowledge that they are aware of their responsibilities and verify that they will comply with security policy. This requires that:
  - Staff should have ample opportunity to read and review all policies and regulations for which they will be held accountable.
  - Staff should be provided an appropriate forum for clarifying questions or concerns they may have about the organization's expectations.
  - Staff should not be given access to the system until a signed agreement is accounted for and maintained in a safe place.

All new employees should be expected to meet the organization's security requirements and procedures as a part of their job description. Once hired, new employees should be informed of, and trained on, security policy as a part of their initial orientation in order to impress the importance of security upon them.

Without proof that an employee agreed to abide by security regulations, the sometimes necessary tasks of reprimanding, dismissing, or even prosecuting security violators can be difficult to pursue.



A Special Note on Outsiders

Outsiders (e.g., repair technicians, consultants, and temporary help) and outside organizations (e.g., other departments, other educational institutions, and contractors) with access to your system should also sign agreements that require them to respect and maintain the confidentiality of your information. But be careful not to share more about your security operation with outsiders than is necessary. Even apparently harmless warnings about what to expect of your defenses can give a skilled intruder

Outside organizations should be expected to guarantee (via binding agreements) that they and their employees will use and secure shared information appropriately.

an edge in tampering with your system. Instead, limit security briefings to those levels required to (1) keep them from breaching your defenses, (2) impress upon them that you are serious about protecting your system assets, and (3) ensure that they handle your assets in a secure manner.

Having said this, sharing general news with the public—parents, local organizations, business partners, and lawmakers to name few—about your organization's commitment to securing confidential information can instill a feeling of confidence throughout your organization and community.

Closing Thoughts on Policy

The incredible pace of technological innovations requires that all security policies be reviewed on a frequent basis. How frequently? That depends on your organization's needs and technological savvy. Generally speaking, however, each new technological change has the potential to necessitate a corresponding policy change—so it is a good rule to review all organizational policies (security or otherwise) annually at a minimum.

Policy Development and Implementation Checklist

While it may be tempting to refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement security policy throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 3

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points for Policy Development and Implementation	Page
		1) Are the findings of the organization's risk assessment (see Chapter 2) available?	29
		2) Have staff who represent a range of job levels and types been included in the security policy development process?	29
		3) Have security-related practices, agreements, and arrangements in other organizations been reviewed to ensure that organizational policy is in line with those in comparable institutions and potential or actual trading partners?	30
		4) Has appropriate and meaningful support/reference information been provided within the policy itself (see checklist under "What to Include")?	30
		5) Has policy been written in a way that can be understood and appreciated by staff?	30

		6) Have policy goals and objectives been translated into organizational security regulations that are designed to modify staff behavior?	31
		7) Has an empowered and committed administrator been specifically assigned to be accountable for security (see also Chapter 4)?	31
		8) Have staff received security training that was specifically tailored to their needs (see also Chapter 10)?	31
		9) Have organizational needs and expectations been communicated to staff in both initial and ongoing ways (see checklist of recommended strategies)?	32
		10) Are security regulations enforced equally at all levels of the organization?	32
		11) Have staff been informed of their security roles and responsibilities in writing?	33
		12) Have security issues been included as a part of employee performance reviews?	33
		13) Is adequate time provided for reading and reviewing Security Agreements before employees and outsiders are required to sign and submit them?	33
		14) Is an appropriate forum provided for clarifying concerns and answering questions about Security Agreements before employees and outsiders are required to sign and submit them?	33
		15) Are all new employees trained on their security roles, responsibilities, and expectations?	33
		16) Are outsiders (e.g., repair technicians) and outside organizations required to sign Security Agreements to acknowledge that they are aware of their responsibilities and will abide by the organization's security rules?	33
		17) Has news of the organization's commitment to security been shared with the general public as appropriate?	34
		18) Are security policies reviewed annually at a minimum?	34

No doctrine, however high, however true, can make men happy until it is translated into life!

—Henry van Dyke

CHAPTER 4

Security Management

CHAPTER 4 IN A NUTSHELL:

Introduction to Security Management pg 37
Commonly Asked Questions pg 38
Nurturing Support within the Organization pg 39
- Garnering Administrator Support pg 39
- Ensuring User Support pg 40

Planning for the Unexpected pg 40
- Security Breach Response Planning pg 41
- Contingency Planning pg 42

Testing and Review pg 45
Implementation and Day-to-Day Maintenance pg 47
- Backups pg 47
- Virus Protection pg 49
- Software Updates pg 49
- User Account Management pg 50
- System Use Monitoring pg 50

Security Management Checklist pg 52

Introduction to Security Management

Because **system** security is the aggregate of individual component security, "system boundaries" must encompass individual **users** and their workstations. But because **personal computers** are just that (personal), staff behavior can't always be dictated without potentially hampering workers' overall productivity. Recall that **security policy** becomes ineffective if it's so restrictive that legitimate user **access** is threatened. Thus, a key to successful security implementation is finding a reasonable balance between system protection and user autonomy and convenience.

Effective security strikes a balance between protection and convenience.

The person responsible for finding that balance and actively promoting organizational security is the security manager. Security management consists of nurturing a security-conscious organizational culture, developing tangible procedures to support security, and managing the myriad of pieces that make up the system. The security manager ensures that administration and staff are aware of their security roles, support security efforts, and are willing to tolerate the minor inconveniences that are inevitably a part of system change and improvement. After all, if personnel circumvent security procedures (e.g., write down **passwords,** share

accounts, and disable **virus**-checking **software**), they put the entire system at **risk.**

Effective system security depends on creating a workplace environment and organizational structure where management understands and fully supports security efforts, and users are encouraged to exercise caution. The security manager leads this effort.

A security manager must:

1) Communicate to staff that protecting the system is not only in the organization's interests, but also in the best interest of users.

2) Increase staff awareness of security issues.

3) Provide for appropriate staff security training.

4) Monitor user activity to assess security implementation.

Commonly Asked Questions

Q. ***Can an organization make do without hiring a security manager?***

A. Yes, but while a security manager doesn't always need to be hired (especially in smaller organizations), someone must perform the functions of security management all the same. Many organizations prefer to hire a systems administrator and include security management as one of his or her primary duties. This is an acceptable strategy as long as the administrator has sufficient time to dedicate to security management. If, however, routine administrative functions take up a considerable part of the administrator's work day, then the organization will be better served by having someone who is able to focus on system security.

Q. ***Would assigning a top educational administrator to the security manager role show commitment to system security?***

A. Not necessarily. Although top administrators are often entrusted with sufficient authority to be effective security managers, it is quite possible that they do not possess the technical expertise necessary for the job. Security managers are responsible for operationalizing all aspects of system security—a task that requires significant technical competence. A secondary, but important, consideration is that managing system security can demand a great deal of time—time that policy-makers and other top administrators may be unable to devote given their other essential duties. While it is imperative that top administrators are actively committed to security effectiveness, in most cases it makes sense that the day-to-day administration of system security be assigned to a security/systems professional.

Q. ***Where does the security manager fit into the organizational hierarchy?***

A. Just as the title implies, security managers and system administrators are most often considered to serve in a management capacity. The important tasks of developing security regulations, training staff, and monitoring implementation require that the security manager be vested

with substantial authority. While the security manager is not to be confused with a superintendent or principal, he or she should be considered to be the system "boss." If the security manager is not able to confidently address security miscues at even the highest levels of the organizational hierarchy, protecting system **resources** adequately becomes an impossibility.

Nurturing Support within the Organization

Even when an organization is committed to improving its information security, security managers often find themselves having to work harder than should be necessary to remind staff of the importance of each step in the security process. Fielding questions about the necessity of sometimes burdensome procedures or the expense of technical and training initiatives is an inevitable but important part of the security manager's job. Make no mistake about it, the security manager must not only administer security policy but must also champion it.

Garnering Administrator Support

Support for security at the managerial level is essential because security planning must be aligned within the context of greater organizational goals. Management must make sure that the organization's broader plans are adequately considered and that security policy conforms to existing rules, regulations, and laws to which the organization is subject—not to mention that adequate funding is budgeted. After all, every dollar that is invested in security, as necessary as it surely is, takes a dollar away from some other activity.

While **technical support staff** may have the best understanding of the ramifications of given technology initiatives, only users have the opportunity to implement policies and management the power to enforce them—and policies that are neither implemented nor enforced are worthless. Real security requires strong, visible support from senior management as a group, as well as personal accountability and exemplary behavior from individual managers. If management ignores or circumvents security procedures, others will do likewise.

Security must be a joint effort between decision-makers, technical staff, and all other personnel.

It Really Happens!

Now Melissa was doing it too!

It just drove Carl crazy. First it was Dr. Dawson who flouted security regulations—but what more was Carl to do after his polite reminders about security policies had been ignored by the Superintendent? Then the Deputy, Dr. Cosgrove, began dismissing the policies as well. Soon both assistant superintendents had decided that they, too, need not comply with inconvenient security regulations. And now it had finally reached Melissa, the executive secretary. Carl didn't blame her—of course she wasn't going to play by the rules when no one else in her office did. But as the security manager, Carl was worried that when word got out that Melissa no longer changed her password regularly or used a screensaver, the rest of the support staff would quit following regulations as well. And from there it was a slippery slope until staff in the schools realized that the central office wasn't following agreed-upon security policies. At this pace, Carl knew it wouldn't take long for the district's entire investment in system security to unravel.

Management can encourage an atmosphere of security, or they can undermine it—their behavior in large part determines whether staff who are meticulous about security are considered to be the oddballs, or the norm.

Employees also have an ethical responsibility to maintain the security of confidential information entrusted to them.

Ensuring User Support

Computers and **networks** are valuable tools to their users. Many people rely on them every day to help perform their jobs more efficiently. When computer resources are not available, fulfilling job requirements can become considerably more difficult. One important role a security manager plays is communicating to staff that protecting the system is in their best interests as well as those of the organization.

Planning for the Unexpected

Traditional computer security frequently relies heavily upon protecting systems from **attack** and minimizing the likelihood of software and equipment failure, but little attention is usually paid to how to handle an attack or failure once it actually occurs. The result is that when a problem does occur, many decisions are made in haste. Often, such decisions reflect this lack of forethought and don't contribute to tracking down the source of the incident, collecting evidence to be used in prosecution efforts, protecting the valuable **information** contained on the system, or preparing for system recovery.

A good policy whenever security is threatened, whether it be a **disk** crash, an external intruder attack, or natural disaster, is to have planned for potential adverse events in advance. The only way to be sure that you have planned in advance for such troubles is to plan now—because you can never predict exactly when a security breach will happen. It could happen in a year, a month, or this afternoon. Planning for emergencies beforehand goes beyond "good policy." There is no substitute for security breach response planning and other more overarching **contingency planning**.

It Really Happens!

The district's backup drive finally broke beyond repair. But Rita, the security manager, was prepared for the eventuality, and quickly produced a copy of a maintenance contract with her vendor that covered exactly this type of event. She called the sales representative and was told that she'd receive a replacement drive within 48 hours. She said that would be fine because the system wasn't due for another complete backup for three more days. Two days later the replacement part arrived as promised, but, to the sales representative's chagrin, it wasn't compatible with the district's system—the wrong part had been sent! Remarkably, Rita maintained her composure as the salesman told her that despite his unyielding efforts to correct the mistake, a new part couldn't possibly reach her rural site for another 48 hours. They'd have to postpone the backup cycle. "Not necessarily," Rita replied with determination.

Ten minutes later Rita was on her way to the County Office Building. Two years earlier she had collaborated with the County Administrator before purchasing technology for the district. The two had agreed to buy compatible equipment that could be shared if an emergency ever arose. While Rita acknowledged that she wasn't quite facing a dire emergency, borrowing the county's backup drive for an evening was a fairly simple procedure—and was exactly what she was going to do to prevent a delay in her backup routine. All of her advanced planning was finally paying off.

Security Breach Response Planning

There are three common responses to an attack on an information system: "protect and proceed," "pursue and prosecute," and "panic and pray." Either of the first two strategies, while clearly opposite in design, can be appropriate depending on the nature of the security breach and the philosophy of the organization. The third approach, "panic and pray," while unfortunately more common than the first two, is never an effective response. In fact, the entire rationale for contingency planning is to minimize the need for panic and prayer in the event of a security incident.

Possible responses to an attack:

1. Protect and Proceed
2. Pursue and Prosecute
3. Panic and Pray

The primary goal of "Protect and Proceed" is the preservation of site assets and the timely return to normal activities.

The primary goal of "Protect and Prosecute" is the identification of intruders and the gathering of evidence of all unauthorized activities.

▶ **Protect and Proceed.** If management fears that the site is particularly vulnerable to attack, it may choose a "protect and proceed" strategy. Upon detection of an attack, attempts are made to actively interfere with the intruder's penetration, prevent further encroachment, and begin immediate damage assessment and recovery. This process may involve shutting down facilities, closing off access to the network, or other drastic measures. The drawback is that unless the intruder is identified directly, he, she, or it may come back into the site via a different path, or may attack another site.

▶ **Pursue and Prosecute.** This alternative to the "protect and proceed" approach adopts the opposite philosophy and goals. Here, the primary goal is to allow intruders to continue to access the system until they can be identified and have evidence of their unauthorized activities gathered against them. While this approach is endorsed by law enforcement agencies and prosecutors because of the evidence it can provide, the major drawback is that the system and its information remain open to potential damage while the organization is trying to identify the source and collect its evidence.

Careful consideration must be given to both of these security breach response philosophies by site management. It is imperative that forethought and planning take place before a problem occurs or else staff may not know how to respond in the event of a real emergency: to protect and proceed, or pursue and prosecute? In fact, the strategy eventually adopted might even be one of "it depends upon the circumstances." For example, an education organization might be willing to accept the additional risks of allowing an intruder to access financial records (that have been properly backed up) while he or she is incriminating him- or herself and being identified. On the other hand, the organization might decide that **threats** that access confidential student records must be thwarted immediately because the potential costs of disclosure are not worth the benefits of capturing the intruder. Regardless of the approach selected, the pros and cons must be examined thoroughly by policy-makers, and users must be made aware of their responsibilities.

Another decision that management must make concerns any distinctions it chooses to make about different types of unauthorized users. Sites may find it helpful to define who it considers to be "insiders" and "outsiders" by referring to administrative, legal, or political boundaries. These boundaries imply what type of action should be taken to reprimand an offending party—from written censure to pressing legal charges. Security plans need to spell out these options and how an appropriate response will be determined if someone is caught behaving in an unauthorized manner.

Prosecution is not the only possible outcome when an intruder is identified. If the culprit is an employee or a student, the organization may choose to take internal disciplinary action.

Security plans should also include procedures for interaction with outside organizations, including law enforcement agencies and other security support sites. The procedures should state who is authorized to make such contact and how it should be handled. Contact information for security support organizations can be found in Appendix E.

Contingency Planning

Hard drives will crash, electrical surges will zap **data,** and **files** will be erased accidentally. General system security (Chapters 5-9) is designed and implemented to protect an organization from these disturbing events. But as valuable as locks, **virus scanners, disk labels**, and passwords can be, if a fire, flood, or sophisticated intruder knocks at your door uninvited, be prepared for trouble.

Make no mistake about the term contingency planning—events that could happen *will* happen, it's just a matter of when.

Contingency planning does not protect the organization from a threat but, instead, explicitly details what is to happen if (when) there is a penetration or the system goes down. It prepares the organization for recovery from a breach in security as quickly and efficiently as possible. In fact, another term for contingency-type planning is **recovery planning.** Planning for recovery from loss or downtime is not pessimistic as much as it is realistic.

For those in the world who are not invincible (read "everyone"), being prepared to overcome the unpredictable is wise and necessary.

Contingency planning can be complex and detailed; after all, it amounts to a blueprint for jump-starting the most important aspects of the organization from scratch and, perhaps, even at another site—all during or, at best, immediately after a catastrophe has struck. The following outline includes recommended steps and considerations for effectively and completely preparing a contingency plan. As with all other guidelines offered in this document, each organization (and its security manager and policy-makers) will need to consider these recommendations and customize them to meet their unique needs.

- Be inclusive when building the contingency planning team by including:[12]
  - Key policy-makers
  - Building management
  - End-users
  - Local authorities
  - The security manager
  - **Technical support**
  - Other representative staff
  - Key outside contacts (e.g., contractors and suppliers)
- Obtain and/or approximate:[13]
  - An exhaustive list of critical activities performed within the organization (as should be identified in your **risk assessment**)
  - An accurate estimate of the minimum space and equipment necessary for restoring essential operations
  - A time frame for starting initial operations after a security incident
  - A list of key personnel and their responsibilities

Contingency planning should be as specific as possible: If threat "a" happens, the organization will respond by doing "b"; if "c" happens, it will do "d".

Perform and/or delegate the following duties as part of the development of a contingency plan:[4]

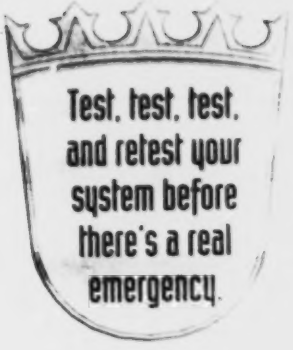
- Create an inventory of all assets, including information (data), software, **hardware,** documentation and supplies—include item by item, the manufacturer's name, model, serial number, and other supporting evidence. Perhaps videotape your facility, including close-ups. Keep it up-to-date and don't forget **peripherals.**
- Set up reciprocal agreements with comparable organizations to share each other's equipment in the event of an emergency at one site (e.g., school district to school district, school district to state department, school district to school, school to local nonprofit). The key is that you have compatible equipment requirements (e.g., MAC to MAC or Windows to Windows).
- Make plans to procure hardware, software, and other equipment as necessary to ensure that mission-critical activities are resumed with minimal delay. Keep in mind that old equipment that you have replaced may no longer ideally meet your needs, but might suffice in a pinch if it still meets your minimum requirements.
- Establish contractual agreements with "hot" and "cold" **backup** sites as appropriate.

▶ A **"hot" site** is an **off-site** facility that includes computers, backed up data, etc. (everything necessary for resuming operations)

▶ A **"cold" site** is an off-site facility that includes everything necessary for resuming operations with the exception of actual computers (if some delay is acceptable, then the expense can be incurred when and only when necessary)

- Identify alternative meeting and start-up locations to be used in case regular facilities are damaged or destroyed.
- Prepare directions to all off-site locations (if and when moving off-site is actually required).
- Establish procedures for obtaining off-site backup records (i.e., who, what, where, how, and under whose direction).
- Gather and safeguard contact information and procedures for communicating with key personnel, suppliers, and other important contacts.
- Arrange with manufacturers to provide priority delivery of emergency orders.
- Locate support resources that might be needed (e.g., equipment repair, trucking, and cleaning companies).
- Establish emergency agreements with data recovery specialists.
- Arrange for uninterrupted site security with local police and fire departments.

- Specify the following within the plan:[15]
  - Individual roles and responsibilities—by name and job title so that everyone knows exactly what needs to be done
  - Actions to be taken in advance of an occurrence or undesirable event
  - Actions to be taken at the onset of an undesirable event to limit damage, loss, and compromise
  - Actions to be taken to restore critical **functions**
  - Actions to be taken to reestablish normal operations

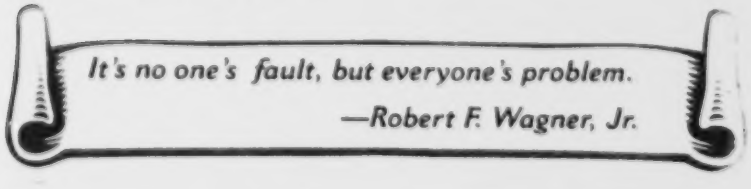


- Test the plan:
  - Test the plan frequently and completely.
  - Analyze test results to determine further needs (e.g., more training and better backup storage).

Periodically try to restore files that have been backed up (be sure to make secondary backups so that you are not risking your only backup copy of the data, but otherwise make the process identical to a real emergency).

- Deal with damage appropriately:
  - If a disaster actually occurs, document all costs (even interim assessment costs) and videotape the damage (to serve as proof of loss).
  - Don't do anything about water damage to technical equipment except immediately contact professional recovery technicians.
  - Be prepared to overcome downtime on your own—insurance settlements can take time to be resolved. Once settled, rebuilding, repurchasing, and reinstalling can take even more time, so don't expect that anything short of being completely prepared will get your office rolling again in a reasonable amount of time.

- Give consideration to other significant issues:
  - Don't make the plan unnecessarily complicated.
  - Make one individual responsible for maintaining the plan, but have it structured so that others are authorized and prepared to implement it if needed.
  - Keep the plan in a secure but convenient location so that it can be accessed as needed.
  - Update the plan regularly and whenever changes are made to your system.
  - Recognize that people *always* come first (before equipment, information, or mission).



This anecdote may sound far-fetched, but something remarkably similar was reported to have happened after the 1996 California earthquake.

It Really Happens!

The Great Quake, as it was soon called, took everyone by surprise—including the regional education agency that had been compiling student records for the state legislature for more than two months. Don Jones was in charge of the project and found himself in quite a predicament. Luckily, or unluckily depending on the outcome of his actions, he didn't think about what he was about to do—he just ran back into the burning building to get a copy of his backup data tapes. He returned to an astonished group of co-workers who were amazed that he would, quite literally, risk his life to protect "his" data. He made it out alive, so he might say that it was worth the risk, but wouldn't it have been easier to have just practiced off-site storage?

Testing and Review

Most organizations undergo some sort of annual financial **auditing** as a regular part of their fiscal life. So, too, are **security audits** an important part of running any computing environment. A complete security audit should include an examination of any policies that affect or are affected by system security, as well as a thorough test of each mechanism that is in place to enforce said policies. After all, a plan isn't much good if it can't be implemented—and the only way to really be sure that security policies and mechanisms are being implemented properly is through extensive testing (or during a real emergency, at which point it is too late to correct shortcomings).

When a threat or disaster is actually happening is not the time to discover the meaning of the phrase "a false sense of security."

Don't let your organization contribute to the numerous stories of contingency plans that failed because of a minor oversight that easily could have been remedied, but wasn't identified until it was too late.

Although **security drills** can't be scheduled every day of the week without seriously affecting office productivity (and probably morale), they should be conducted as frequently as is necessary to determine that security procedures are being implemented effectively. What kind of drills? Well, if your risk assessment (see Chapter 2) identifies a particular type of natural disaster as a primary threat to your organization, then a drill based on that scenario could be constructed (e.g., a test to verify your backup and recovery mechanisms after an earthquake). On the other hand, if your greatest threat is from external intruders attempting to penetrate your system, a drill might be conducted that simulates a **hacker** attack in order to observe access **countermeasures** in action.

Keep in mind that there are limits to reasonable testing. The purpose of testing is to verify that security procedures are being implemented properly and meet critical policy goals, not to prove the absoluteness of every aspect of the system and policy.

It Really Happens!

City Schools committed itself to top-rate system security. It assigned a staff member to serve as a full-time security manager, purchased state-of-the-art backup equipment, and refurbished an old building it owned on the edge of town to serve as off-site storage for its backup tapes. The security manager, having attended numerous technology and security conferences to keep abreast of his job responsibilities, took pride in his system and tested every step of his backup procedures right up until the tapes hit the shelves at the off-site storage facility. To the best of the manager's knowledge, security drills had proven time and again that the system could truly be trusted. One night, as the manager lay in bed thinking about how wonderful the City Schools security system was, he realized that he'd never actually reloaded backup tapes from off-site storage. He was, of course, very confident that the facility (with its fire-retardant renovations, anti-static carpeting, and full-time security guard) was secure, but acknowledged that he couldn't be sure until he actually tested it.

The next morning, he went to the facility, checked in with the security guard, entered the combination to unlock the door, and signed out a sample tape. He took it to his office and tried to reload it on a stand-alone "test" computer, but, to his great surprise, found that the tape held no data. He immediately returned to the storage facility to withdraw another tape but again, upon trying to read the data, found that there were no files.

Quicker than a flash, the security manager called in a team of high-tech security consultants to diagnose his problem. He showed them his records of test after test and drill after drill that verified that all pre-storage steps to backing up the data were being implemented properly. The specialists were convinced that the off-site facility was the place to begin the investigation. As they approached the building, the security manager mentioned that while he hadn't thought to budget for the high hourly charges of the expert consultants, they should take whatever time they needed to figure out the problem because he wanted that backup system running properly. To this, the lead consultant replied as he walked toward the door, "Well, in that case I think that I've got some good news and some bad news to tell you. The good news is that I've already identified your problem and will only have to charge you for one hour's work."

"That is good news," the manager responded. "But what's the bad news?"

"The bad news is that electrical transformer behind the storage facility. Unless you have lead walls, it's emanating enough residual electricity to erase every tape you have in the building. You're going to have to move your storage site."

"But we have a very secure site here," the manager contended desperately. "It has a security guard, a state-of-the-art sprinkler system, and anti-static carpeting."

"And it also has a giant, tape erasing, electrical plant in its back yard. I'm sorry, but this site will never be secure. Every backup tape that gets within 50 feet of the building is going to have all of its data erased. But look at the bright side—while you may have lost the investment in the facility, at least you found all this out before you really needed the backed up data. Take last night's tapes to another storage location and you should be okay."

Although security can't be tested each day, testing must be performed frequently enough to verify the effectiveness of security initiatives.

If full-fledged security drills prove to be too time-consuming and disruptive to normal operations to be implemented on a large scale, consider testing individual facets of the security system one at a time. Backup procedures can be examined to make sure that data can be recovered from storage **tapes.** Log files can be checked to make sure that information that is supposed to be maintained has been done so accurately. And other features of the system can be evaluated and analyzed as well. When a security drill is performed, great care should be given to devising the test. It is important to clearly identify what is being tested, how the test will be conducted, and what results are to be expected. All aspects of this process should be documented and included in, or as an adjunct to, the security policy.

Who performs security audits and drills?

1) The organization's security professional(s)
2) Employee teams (peer reviewers from within the organization)
3) External reviewer teams (from cooperatives, consortia, or other partner organizations)
4) Hired external expert security consultants

Implementation and Day-to-Day Maintenance

Security is more than keeping hackers and other trouble-makers out of your system. It involves a host of internal practices that serve to protect information in the case of system or **disk** failure. Some of the main activities security managers engage in on a day-to-day basis include administering backup and virus protection mechanisms, staying abreast of software updates, managing user accounts, and monitoring system activity.

Backups

It is almost impossible to over-emphasize the need for a good backup strategy. System backups not only protect the organization in the event of hardware failure or accidental deletions, but they also protect staff against unauthorized or accidental changes made to file contents. If an error is ever made (and we all know that they are), having the option of accessing an unaltered backup can be very appealing. But reaching into those archives is a viable strategy only when backup files have been made properly—a backup of a file that contains the errors and/or viruses you are trying to eliminate usually isn't very helpful. Similarly, backup files need to be created at appropriate intervals and themselves must be well protected from damage and destruction.

Recommended practices concerning actual backup procedures are included in Chapter 6.

Which type of backup strategy makes sense for your organization? That depends on the types and number of files in the system, the level of technical expertise within the organization, and the organization's commitment to security—information that can be found in the results of a well-executed risk assessment (see Chapter 2). Even after needs unique to the organization have been identified, however, there are several more overarching issues that need to be considered before establishing backup plans:

1) What amount of exposure to data loss can your organization comfortably tolerate?
2) How old is your equipment? How reliable is it?
3) What is the nature of your workplace? Do you process new data everyday?

To further evaluate the type of backup strategy that will best meet your organization's needs, also weigh the following factors:[48]

1) The time and effort required to make changes to the files:

If changes to the file take only a little time, backing up those changes may not be imperative. If the changes require a great deal of work (e.g., entering data collected from a long form), don't risk that effort and instead back it up frequently.

2) The time and effort required to back up the files:

If the actual backing up process requires little effort, why put it off? If it is time consuming, be more aware of proper timing.

3) The value of the data:

If the data are particularly valuable, back them up more often. If not, frequent backup may be less necessary.

4) The rate of file change:

If a document changes rapidly (e.g., because of the operator's speed in data entry), more frequent backup is probably needed.

You may choose a combination of complete and partial backup routines. However, when initiating any system, a complete backup should first be done to serve as a reference point.

In general, there are three types of backup strategies:

1) A *complete* backup—backing up your *entire* hard drive. The advantage of this strategy is its completeness; you will get a snapshot of all your hard disk's contents.

2) A *partial* backup—only backing up *selected* directories. This is useful and efficient if your work is concentrated in a specific area of your hard disk.

3) An *incremental* backup—only backing up those files that have been *changed* since the last backup. It means using backup software to scan the files to see if they have been changed since the last backup cycle. If so, the file is saved; if not, the previous backup is maintained.

Above all, devise a backup strategy that is realistic for your organization's setting.

So how do all of these factors get synthesized into an effective strategy for meeting an organization's needs? The answer is simple: use the information available in order to devise a backup plan that is most likely to be implemented. Whatever the solution might be, be creative enough to develop the strategy that is most likely to ensure that your data gets backed up. It is imperative to establish realistic policies based on your agency's environment.

In any case, set a backup schedule that fits your agency's needs and work style and stick with it. Here are a few examples of common backup routines:

- Twice daily: partial at noon, full at end of day
- Once daily: full backup at end of day
- Three times weekly: full backup at end of every other day
- Twice weekly: full backup Tuesday, partial on Thursday
- Once a week: full backup
- Monthly: full backup

A last major planning issue to consider is what to do with backup files once they have been created. The choice of backup location depends on the agency's needs, resources, and ability to secure its physical structure (see Chapter 5). Any single option, or mixture of options, can be chosen as long as they meet the site's needs and have a realistic chance of being implemented. Backup storage options include:

Option A In the same room—great for easily recovering files after data loss, but bad if a threat gets "in" the room.

Option B In the same building—less convenient for correcting mistakes, but physical separation increases security as a single event is less likely to damage everything.

Option C In a secure, off-site location—not convenient at all for quick data recovery, but excellent for protection if maintained in a secure facility.

Option C, "In a secure off-site location," is the best option from purely a security perspective. See Chapter 5 for recommendations on securing a location.

Like all security decisions, selecting a location for off-site storage facilities should be based on risk assessment findings. If, for example, risk assessment shows that an earthquake is the threat of chief concern, locating an off-site storage facility 100 miles away but along the same fault line makes little sense. Similarly, if risk assessment identifies flood as a paramount threat, the location of off-site storage should be outside the same flood plain.

Virus Protection

Any machine that is connected to a network or that interacts with others via **diskettes** or a **modem** is vulnerable to **rogue programs:** computer viruses, **worms, Trojan horses,** and the like. It is the security manager's duty to develop and monitor procedures for preventing viruses and other rogue programs from infiltrating the system. As a rule of thumb, no diskette from outside the system (including brand name, shrink-wrapped software) should ever be used on a system machine without first having been scanned by an up-to-date **antivirus** program.

See Chapter 6 for more specific guidelines about combating viruses and other rogue programming.

The most effective protection against a virus is having a clean, up-to-date backup file.

Software Updates

It goes without saying that computer systems have **bugs.** Even **operating systems,** upon which we depend for so much of the protection of our information, have bugs. Because of this, software publishers **release** updates on a frequent basis. Often these updates are, in fact, plugs for holes in the software's security that have been discovered. It is important that whenever these bugs are identified, the system manager takes all action possible to remedy them as soon as possible in order to minimize exposure.

A corollary to the "bug problem" deals with the source for obtaining **upgrades** to software. Many computer systems and software packages come with support from the manufacturer or supplier. Remedies that come directly from such a source tend to be trustworthy and can usually be

Bug \'bəg\ - any of a near countless number of species of creepy, crawly insects, or, more commonly, unexpected programming errors in computer software.

implemented fairly quickly after receipt (and proper testing no matter the source). Other sources, such as software posted on **Internet** sites, must be scrutinized more closely.

As a general rule, trust manufacturer upgrades more than those that are posted on the Internet.

User Account Management

Effective security demands "checks and balances" so that every user, including the system administrator and security manager, is accountable for system activity—no one should be able to print his or her own paycheck without being monitored.

As stated throughout this chapter, a single person needs to have primary responsibility for an information system. For this person, the security manager or systems administrator, to effectively supervise the system, he or she needs to have access to all system components and files—access that is commonly referred to as "system administrator privileges." It is generally considered to be good practice to share system administrator access privileges with someone other than the system administrator, if for no other reason than to have emergency system access should the administrator ever become unavailable. But, having said this, such total access also requires total accountability, and should be limited to the fewest number of staff as is necessary to keep the system secure—after all, each person with total system access has the ability to override any and all security features.

Users other than the system manager (and an accountable replacement in case of emergency) should be given access to the system based solely on their job needs. Restricting user access minimizes the opportunities for accidents and other possibly inappropriate actions (see Chapter 8). Through the use of user accounts, each authorized user is identified before accessing the system, and any action that is made by that user is classified as such.

Users should be given access only to files and systems that they need to do their jobs, and nothing more.

System Use Monitoring

To recognize deviations from normal system use, the manager must understand how the system behaves when it is running properly.

System monitoring can be done by either the security manager or by software designed specifically for that purpose. Monitoring a system involves looking at all aspects of the system, identifying patterns of regular use, and searching for anything unusual. Most operating systems store information about system use in special files referred to as log files. Examination of these log files on a regular basis is often the first line of defense in detecting unauthorized use of the system. System managers should:

- Compare lists of currently logged-in users and past **log-in** histories. Most users typically log in and out at roughly the same time each day. An account logged in outside the "normal" time for the account may be a sign of unauthorized activity and require investigation and explanation.
- Check system logs for unusual error messages. For example, a large number of failed log-in attempts in a short period of time may indicate that someone is trying to guess passwords.

It Really Happens!

Steve was serious about the security of his school's computer system. And although some folks may have thought that he was perhaps too serious, it didn't stop him from making them toe the security line all the same. He was a no-nonsense kind of security manager.

When he noticed some extraordinarily odd system activity one afternoon during his daily (but randomly timed) monitoring operations, he was fast on the trail of the troublemaker. Steve knew he was an efficient security manager, but he surprised even himself by so quickly tracing the violations back to Mrs. Todd, the fifth-grade teacher. He should have known to never have trusted Mrs. Todd. No one could be that nice—it had to be a ruse.

Steve marched down the hall and through the door into the empty classroom in time to find the culprit still seated at her computer. He could barely control himself, "What in the world do you think you're doing? You could lose your job for hacking my system. In fact, I'm going to do my best to see that you do!"

As Steve could have predicted, Mrs. Todd denied that she had done anything improper. "But, Mr. Johnson, what are you talking about?... And please don't use that tone with me."

"Tone?" Steve replied in amazement. "You're lucky that all I use is 'tone' with you. Now let me see what you're doing here." He walked behind Mrs. Todd's desk and looked at her monitor screen. "Hmm," Steve thought out loud, surprised to see that she was working on the electronic grade book that was on her own hard drive and didn't require being logged on to the network. "What were you doing before I got here? Were you on the network?"

Mrs. Todd looked puzzled, "No, I've been in my grade book since the children left. Why?"

Before Steve could continue with his interrogation, Mrs. Yow, the Principal, charged into the room. "What is all the commotion about, Steve? I could hear you hollering half-way down the hall."

"I caught Mrs. Todd tampering with the report card files on the network. It's a serious offense to our security system."

Mrs. Todd was quick to defend herself. "He did no such thing, Mrs. Yow. He couldn't have caught me doing that because I would never do such a thing. Look, I'm working on my own grade book."

Steve was surprised that Mrs. Todd was able to maintain such a straight face when he had caught her nearly red-handed. But before he could say anything, Mrs. Yow reached for Mrs. Todd's keyboard. She hit a few function keys and clicked the mouse once or twice. Steve could tell that she was pulling up an audit trail of the computer's use. He loved having a principal who knew her way around the equipment!

"Steve," Mrs. Yow asked, "what time did the violation take place?"

"Three o'clock," he replied, "right after last period. That's when Mrs. Todd said she got on the computer. Quite a coincidence, huh?"

> While the security manager is responsible for monitoring user activity, doing so becomes much more feasible when working with and not against the staff.

The principal stared at him, "It must have been a coincidence, because the audit trail shows that she's been in her grade book file since 3:02 p.m. No activity before that since eight o'clock this morning." Mrs. Yow frowned at Steve before looking apologetically at the fifth-grade teacher, "I'm sorry Mrs. Todd. He may get carried away sometimes, but he does have a big job in keeping our network safe." She looked back at Steve, "Did you really need to make such a scene when you weren't even sure that you were accusing the right person?"

Steve tried to reply, but Mrs. Todd cut him off. "That's okay, he must have really thought he had found the culprit." She laughed, "Me, a computer hacker, isn't that a story?"

Steve looked at the woman who now defended him. Just moments earlier, he had wrongly accused her of hacking and had threatened her job. So, she might really be that sweet after all.

"Come on, Steve," Mrs. Yow finally said, breaking the silence, "we've got a hacker to identify. This time, no going off half-cocked with accusations until we know what we're talking about."

Post-script: Over the next two weeks, Steve and Mrs. Yow monitored a hacker who was masquerading as several different staff members (including Mrs. Yow) and attempting to enter protected report card files. After

much analysis, Steve identified a bug in the password software that allowed the hacker to misrepresent himself as an authorized user. Once this was accomplished, they were able to trace the unauthorized activities back to the machine from which the intruder was working—and, subsequently, were able to catch the eighth-grade student who was trying to pull off the charade. After dealing with the troublesome student appropriately (during which time Steve let Mrs. Yow do most of the talking), Steve again apologized to sweet Mrs. Todd for his unwarranted accusations and unprofessional behavior.

The task of systems monitoring is not as daunting as it may seem. Security managers can execute many monitoring tasks periodically throughout the day during even the briefest of free moments (e.g., while waiting on hold on the telephone). By executing the commands frequently, the manager will rapidly become familiar with seeing "normal" activities and become better able to spot things that are out of the ordinary.

The single most important thing about monitoring system use is that it be done regularly. Picking one day out of the month to monitor the system is not a solid security strategy, since a breach can take place in a matter of hours or even minutes. Only by maintaining a constant vigil can you expect to detect security violations in time to react to them—hence one appeal of monitoring software that, unlike even the most dedicated of administrators, is able to work 24 hours and seven days a week.

Despite the advantages that regular system monitoring provides, some intruders will be aware of the standard log-in mechanisms used by systems they are attacking and will actively attempt to evade these mechanisms. Thus, while regular monitoring is useful in detecting intruders, it does not guarantee that your system is secure and should not be considered an infallible method of detecting unauthorized use.

A Final (But Very Important) Question

Q. ***How does a security manager verify that the system for which he or she is responsible is actually secure?***

A. 1) Read this document and follow the security guidelines as outlined in the checklists at the end of each chapter.

2) Practice, drill, and test each and every security measure being implemented.

Security Management Checklist

While it may be tempting to simply refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement security policy throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 4

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points for Policy Development and Implementation	Page
		1) Has it been communicated to staff that protecting the system is in everyone's best interests?	38
		2) Has an effort been made to increase staff awareness of security issues?	38
		3) Has appropriate staff security training been provided?	38
		4) Are security activities regularly monitored (see Step 14 below)?	38
		5) Has administrator support been garnered?	39
		6) Has user support been sought?	40
		7) Has a security breach response plan been developed?	41
		8) Have contingency plans been developed to deal with significant and probable threats (addressing the issues raised on pages 42-44)?	42
		9) Are response and contingency plans frequently and exhaustively tested?	45
		10) Has a backup plan been developed and implemented?	47
		11) Is a virus protection system in place?	49
		12) Are software updates tracked?	49
		13) Are user accounts managed appropriately?	50
		14) Is system use monitored appropriately?	50

CHAPTER 5

Protecting Your System: Physical Security

CHAPTER 5 IN A NUTSHELL:

Introduction to Physical Security	pg 55
Commonly Asked Questions	pg 55
Policy Issues	pg 56
Physical Security Countermeasures	pg 57
Physical Security Checklist	pg 63

Introduction to Physical Security

Most people think about locks, bars, alarms, and uniformed guards when they think about security. While these **countermeasures** are by no means the only precautions that need to be considered when trying to secure an information **system,** they are a perfectly logical place to begin. Physical security is a vital part of any security plan and is fundamental to all security efforts—without it, information security (Chapter 6), software security (Chapter 7), user access security (Chapter 8), and network security (Chapter 9) are considerably more difficult, if not impossible, to initiate. Physical security refers to the protection of building sites and equipment (and all **information** and **software** contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

Commonly Asked Questions

Q. ***How can I implement adequate site security when I am stuck in an old and decrepit facility?***

A. Securing your site is usually the result of a series of compromises—what you need versus what you can afford and implement. Ideally, old and unusable buildings are replaced by modern and more serviceable facilities, but that is not always the case in the real world. If you find yourself in this situation, use the **risk assessment** process described in Chapter 2 to identify your **vulnerabilities** and become aware of your preferred security solutions. Implement those solutions that you can, with the understanding that any steps you take make your system that much more secure than it had been. When it comes time to argue for new facilities, documenting those vulnerabilities that were not addressed earlier should contribute to your evidence of need.

Q. *Even if we wanted to implement these physical security guidelines, how would we go about doing so?*

A. Deciding which recommendations to adopt is the most important step. Your risk assessment results should arm you with the information required to make sound decisions. Your findings might even show that not every guideline is required to meet the specific needs of your site (and there will certainly be some variation based on need priorities). Once decided on, however, actually initiating a strategy is often as simple as raising staff awareness and insisting on adherence to regulations. Some strategies might require basic "handyman" skills to install simple equipment (e.g., key locks, fire extinguishers, and surge protectors), while others definitely demand the services of consultants or contractors with special expertise (e.g., window bars, automatic fire equipment, and alarm systems). In any case, if the organization determines that it is necessary and feasible to implement a given security strategy, installing equipment should not require effort beyond routine procedures for completing internal work orders and hiring reputable contractors.

Q. *What if my budget won't allow for hiring full-time security guards?*

A. Hiring full-time guards is only one of many options for dealing with security monitoring activities. Part-time staff on watch during particularly critical periods is another. So are video cameras and the use of other staff (from managers to receptionists) who are trained to monitor security as a part of their duties. The point is that by brainstorming a range of possible **countermeasure** solutions you can come up with several effective ways to monitor your workplace. The key is that the function is being performed. How it is done is secondary—and completely up to the organization and its unique requirements.

Determining countermeasures often requires creativity: don't limit yourself to traditional solutions.

Policy Issues

Physical security requires that building site(s) be safeguarded in a way that minimizes the **risk** of **resource** theft and destruction. To accomplish this, decision-makers must be concerned about building construction, room assignments, emergency procedures, regulations governing equipment placement and use, power supplies, product handling, and relationships with outside contractors and agencies.

The physical plant must be satisfactorily secured to prevent those people who are not authorized to enter the site and use equipment from doing so. A building does not need to feel like a fort to be safe. Well-conceived plans to secure a building can be initiated without adding undue burden on your staff. After all, if they require access, they will receive it—as long as they were aware of, and abide by, the organization's stated security policies and guidelines (see Chapter 3). The only way to ensure this is to demand that before any person is given **access** to your system, they have first signed and returned a valid Security Agreement. This necessary **security policy** is too important to permit exceptions.

Guidelines for security policy development can be found in Chapter 3.

Physical Threats (Examples)

Examples of physical **threats** include:

- Natural events (e.g., floods, earthquakes, and tornados)
- Other environmental conditions (e.g., extreme temperatures, high humidity, heavy rains, and lightning)
- Intentional acts of destruction (e.g., theft, vandalism, and arson)
- Unintentionally destructive acts (e.g., spilled drinks, overloaded electrical outlets, and bad plumbing)

As discussed more completely in Chapter 2, a threat is any action, actor, or event that contributes to risk.

Physical Security Countermeasures

The following countermeasures address physical security concerns that could affect your site(s) and equipment. These strategies are recommended when risk assessment identifies or confirms the need to counter potential breaches in the physical security of your system.

A countermeasure is a step planned and taken in opposition to another act or potential act.

Countermeasures come in a variety of sizes, shapes, and levels of complexity. This document endeavors to describe a range of strategies that are potentially applicable to life in education organizations. In an effort to maintain this focus, those countermeasures that are *unlikely* to be applied in education organizations are *not* included here. If after your risk assessment, for example, your security team determines that your organization requires high-end countermeasures like retinal scanners or voice analyzers, you will need to refer to other security references and perhaps even need to hire a reliable technical consultant.

Select only those countermeasures that meet perceived needs as identified during risk assessment (Chapter 2) and support security policy (Chapter 3).

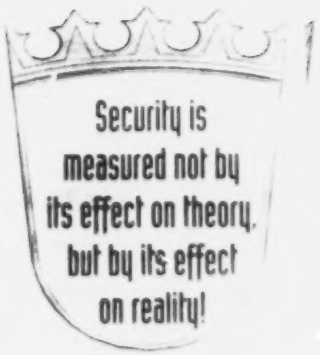
Create a Secure Environment: Building and Room Construction:[17]

- *Don't arouse unnecessary interest in your critical facilities:* A secure room should have "low" visibility (e.g., there should not be signs in front of the building and scattered throughout the hallways announcing "expensive equipment and **sensitive information** this way").
- *Maximize structural protection:* A secure room should have full height walls and fireproof ceilings.
- *Minimize external access (doors):* A secure room should only have one or two doors—they should be solid, fireproof, lockable, and observable by assigned security staff. Doors to the secure room should never be propped open.
- *Minimize external access (windows):* A secure room should not have excessively large windows. All windows should have locks.
- *Maintain locking devices responsibly:* Locking doors and windows can be an effective security strategy as long as appropriate authorities maintain the keys and combinations responsibly. If there is a breach, each compromised lock should be changed.
- *Investigate options other than traditional keyhole locks for securing areas as is reasonable:* Based on the findings from your risk assessment (see Chapter 2), consider alternative physical security

strategies such as window bars, anti-theft **cabling** (i.e., an alarm sounds when any piece of equipment is disconnected from the system), magnetic key cards, and motion detectors.

Recognize that some countermeasures are ideals and may not be feasible if, for example, your organization is housed in an old building.

- *Be prepared for fire emergencies:* In an ideal world, a secure room should be protected from fire by an automatic fire-fighting system. Note that water can damage electronic equipment, so carbon dioxide systems or halogen agents are recommended. If implemented, staff must be trained to use gas masks and other protective equipment. Manual fire fighting equipment (i.e., fire extinguishers) should also be readily available and staff should be properly trained in their use.
- *Maintain a reasonable climate within the room:* A good rule of thumb is that if people are comfortable, then equipment is usually comfortable—but even if people have gone home for the night, room temperature and humidity cannot be allowed to reach extremes (i.e., it should be kept between 50 and 80 degrees Fahrenheit and 20 and 80 percent humidity). Note that it's not freezing temperatures that damage **disks,** but the condensation that forms when they thaw out.
- *Be particularly careful with non-essential materials in a secure computer room:* Technically, this guideline should read "no eating, drinking, or smoking near **computers,**" but it is quite probably impossible to convince staff to implement such a regulation. Other non-essential materials that can cause problems in a secure environment and, therefore, should be eliminated include curtains, reams of paper, and other flammables.



Don't say it if you don't mean it—instituting policies that you don't bother to enforce makes users wonder whether you're serious about other rules as well.

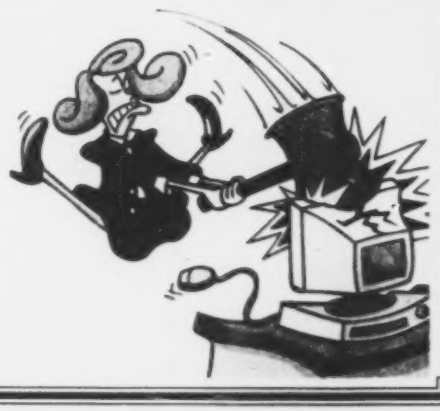
Guard Equipment:

- *Keep **critical systems** separate from **general systems:*** Prioritize equipment based on its criticality and its role in processing sensitive information (see Chapter 2). Store it in secured areas based on those priorities.
- *House computer equipment wisely:* Equipment should not be able to be seen or reached from window and door openings, nor should it be housed near radiators, heating vents, air conditioners, or other duct work. Workstations that do not routinely display sensitive information should always be stored in open, visible spaces to prevent covert use.
- *Protect cabling, plugs, and other wires from foot traffic:* Tripping over loose wires is dangerous to both personnel and equipment.
- *Keep a record of your equipment:* Maintain up-to-date logs of equipment manufacturers, models, and serial numbers in a secure location. Be sure to include a list of all attached **peripheral equipment.** Consider videotaping the equipment (including close-up shots) as well. Such clear evidence of ownership can be helpful when dealing with insurance companies.
- *Maintain and repair equipment:* Have plans in place for emergency repair of critical equipment. Either have a technician who is trained to do repairs on staff or make arrangements with someone who has ready access to the site when repair work is needed. If funds allow, consider setting up **maintenance contracts** for your critical equipment. Local computer suppliers often offer service contracts for equipment they sell, and many workstation and **mainframe** vendors also provide such services. Once you've set up the contract, be sure that contact information is kept readily available. **Technical support** telephone numbers, maintenance contract numbers, customer identification numbers, equipment serial numbers, and mail-in information should be posted or kept in a log book near the system for easy reference. Remember that computer repair technicians may be in a position to access your **confidential information,** so make sure that they know and follow your policies regarding outside employees and contractors who access your system.

Locking critical equipment in a secure closet can be an excellent security strategy if risk assessment findings establish that it is warranted.

Who Needs a Maintenance Contract?

"Percussive maintenance" is the fine art of pounding on a piece of sensitive electronic equipment until it returns to proper working order.



Losing a computer to theft has both financial costs (the **replacement value of the equipment**) and information costs (the files contained on the **hard drive**).

Rebuff Theft:[18]

- *Identify your equipment as yours in an overt way:* Mark your equipment in an obvious, permanent, and easily identifiable way. Use bright (even fluorescent) paint on **keyboards, monitor** backs and sides, and computer bodies. It may decrease the resale value of the components, but thieves cannot remove these types of identifiers as easily as they can adhesive **labels.**
- *Identify your equipment as yours in a covert way:* Label the inside of equipment with the organization's name and contact information to serve as powerful evidence of ownership.
- *Make unauthorized tampering with equipment difficult:* Replace regular body case screws with Allen-type screws or comparable devices that require a special tool (e.g., an Allen wrench) to open them.
- *Limit and monitor access to equipment areas:* Keep an up-to-date list of personnel authorized to access sensitive areas. Never allow equipment to be moved or serviced unless the task is pre-authorized and the service personnel can produce an authentic work order and verify who they are. Require picture or other forms of identification if necessary. Logs of all such activity should be maintained. Staff should be trained to always err on the cautious side (and the organization must support such caution even when it proves to be inconvenient).

Laptops and other expensive equipment that leave the office often never return.

Attend to Portable Equipment and Computers:[19]

- *Never leave a **laptop** computer unattended:* Small, expensive things often disappear very quickly—even more quickly from public places and vehicles!

While the X-ray conveyor belt is the preferred way of transporting a laptop through airport security (compared to subjecting the computer to the magnetic fields of walk-through or wand scanners), it is also a prime place for theft. Thieves love to "inadvertently" pick up the wrong bag and disappear while passengers are fumbling through their pockets to find the loose coins that keep setting off the metal detectors. Use the X-ray conveyor belt, but *never* take your eyes off your laptop!

Require laptop users to read the recommended travel guidelines that should come with the equipment's documentation.

- *Store laptop computers wisely:* Secure laptops in a hotel safe rather than a hotel room, in a hotel room rather than a car, and in a car trunk rather than the back seat.
- *Stow laptop computers appropriately:* Just because a car trunk is safer than its back seat doesn't mean that the laptop won't be damaged by an unsecured tire jack. Even if the machine isn't stolen, it can be ruined all the same. Stow the laptop and its battery safely!
- *Don't leave a laptop computer in a car trunk overnight or for long periods of time:* In cold weather, condensation can form and damage the machine. In warm weather, high temperatures (amplified by the confined space) can also damage **hard drives.**

It Really Happens!

Jack's briefcase was his life. Well, maybe it wasn't his whole life, but it definitely contained the better part of his professional life. It held his grade book, his lesson plans, his master's thesis—all very important things in the world of a middle school teacher.

And it wouldn't be an exaggeration to say that Jack sure was surprised when his life (the briefcase) went up in flames one afternoon in the school cafeteria. He couldn't explain it, but nonetheless he found himself sitting in front of the district technologist trying to do exactly that—explain why his briefcase caught on fire and ruined, among more important things to him, the spare battery he was carrying for the school's laptop computer.

"So," the technologist asked, "you're saying that you're surprised that your briefcase caught on fire? Well, let me tell you, I'm glad that it was only your bag that was damaged. Didn't you know that the exposed terminals of a battery can cause a spark? Didn't you know that any piece of metal, even a paper clip, can serve as the conduit? That's all it takes: an improperly stored battery, a paper clip and anything combustible—and wham, you've got yourself a fire. Your home could have gone up in flames last night because of it. Or your school could have this afternoon. Didn't you know that?"

Jack almost replied that, of course, he hadn't known about all of those dangers, and that the technologist should have warned him about them before he had borrowed the laptop and extra battery. But instead he just shook his head sheepishly. After all, along with his grade book, lesson plans, and master's thesis, he had just burned a $200 dollar laptop battery that didn't belong to him.

Regulate Power Supplies:

- *Be prepared for fluctuations in the electrical power supply:* Do so by (1) plugging all electrical equipment into surge suppressors or electrical power filters; and (2) using Uninterruptible Power Sources (UPSs) to serve as auxiliary electrical supplies to critical equipment in the event of power outages.
- *Protect power supplies from environmental threats:* Consider having a professional electrician design or redesign your electrical system to better withstand fires, floods, and other disasters.
- *Select outlet use carefully:* Although little thought generally goes into plugging equipment into an outlet, machines that draw heavily from a power source can affect, and be affected by, smaller equipment that draws energy from the same outlet.
- *Guard against the negative effects of static electricity in the office place:* Install anti-static carpeting and anti-static pads, use anti-static sprays, and encourage staff to refrain from touching metal and other static-causing agents before using computer equipment.

Pay attention to the manufacturer's recommendations for storing portable computer batteries—they carry live charges and are capable of igniting fires if not handled properly.

Protect Output:

- *Keep photocopiers, fax machines, and scanners in public view:* These types of equipment are very powerful tools for disseminating information—so powerful, in fact, that their use must be monitored.
- *Assign printers to **users** with similar security clearances:* You don't want employees looking at sensitive financial information (e.g., staff salaries) or confidential student information (e.g., individual records) while they are waiting for their documents to print. It is better to dedicate a **printer** to the Director of Finance than to

have sensitive **data** scattered around a general use printer. Don't hesitate to put printers in locked rooms if that is what the situation demands.

- *Label printed information appropriately:* Confidential printouts should be clearly identified as such.
- *Demand suitable security procedures of common carriers when shipping/receiving confidential information:* Mail, delivery, messenger, and courier services should be required to meet your organization's security standards when handling your confidential information.
- *Dispose of confidential waste adequately:* Print copies of confidential information should not be placed in common dumpsters unless shredded. (Comparable requirements for discarding electronic copies of confidential information can be found in Chapter 6.)

It Really Happens!

Dr. Hamilton was everything that a school district could ask for. She was a great visionary, a trusted leader, and an excellent superintendent... but she was terrible with the piles of paper she kept on her desk. Luckily for her and the district, she had an equally competent secretary. Lucy was always one step ahead of Dr. Hamilton with the paperwork. She knew where to find the latest draft of the letter to the Board. She knew which form needed to be completed by when. She knew how many copies of the monthly report needed to be run off.

One afternoon, Dr. Hamilton came running out of her office to Lucy's desk, "You haven't shredded those papers I gave you this morning yet, have you?"

As was always the case, Lucy had, of course, completed the task shortly after it had been handed to her. She told Dr. Hamilton so, and asked what was the matter.

"I think that I accidentally gave you my only copy of the speech I'm giving to the Chamber of Commerce tonight," the distraught woman replied, knowing that she'd never be able to reproduce the outline in time for the meeting.

"Don't worry," Lucy said, beaming with pride that her forethought was about to again pay off, "I make backup copies of every sheet of paper you give me before I turn on that paper shredder. Let's look in my filing cabinet."

Dr. Hamilton let out a deep sigh of relief—Lucy had again saved the day. Suddenly, however, the astute superintendent paused, "What do you mean you make copies of everything I give you before you turn on the paper shredder?"

Don't throw a monkey-wrench into the machinery.
—Philander Johnson

Physical Security Checklist

While it may be tempting to simply refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement security policy throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 5

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points for Physical Security	Page
		Create a Secure Environment: Building and Room Construction	**57**
		1) Does each secure room or facility have low visibility (e.g., no unnecessary signs)?	**57**
		2) Has the room or facility been constructed with full-height walls?	**57**
		3) Has the room or facility been constructed with a fireproof ceiling?	**57**
		4) Are there two or fewer doorways?	**57**
		5) Are doors solid and fireproof?	**57**
		6) Are doors equipped with locks?	**57**
		7) Are window openings to secure areas kept as small as possible?	**57**
		8) Are windows equipped with locks?	**57**
		9) Are keys and combinations to door and window locks secured responsibly?	**57**
		10) Have alternatives to traditional lock and key security measures (e.g., bars, anti-theft cabling, magnetic key cards, and motion detectors) been considered?	**57**

BEST COPY AVAILABLE

		11) Have both automatic and manual fire equipment been properly installed?	58
		12) Are personnel properly trained for fire emergencies?	58
		13) Are acceptable room temperatures always maintained (i.e., between 50 and 80 degrees Fahrenheit)?	58
		14) Are acceptable humidity ranges always maintained (i.e., between 20 and 80 percent)?	58
		15) Are eating, drinking, and smoking regulations in place and enforced?	58
		16) Has all non-essential, potentially flammable, material (e.g., curtains and stacks of computer paper) been removed from secure areas?	58
		Guard Equipment	59
		17) Has equipment been identified as critical or general use, and segregated appropriately?	59
		18) Is equipment housed out of sight and reach from doors and windows, and away from radiators, heating vents, air conditioners, and other duct work?	59
		19) Are plugs, cabling, and other wires protected from foot traffic?	59
		20) Are up-to-date records of all equipment brand names, model names, and serial numbers kept in a secure location?	59
		21) Have qualified technicians (staff or vendors) been identified to repair critical equipment if and when it fails?	59
		22) Has contact information for repair technicians (e.g., telephone numbers, customer numbers, maintenance contract numbers) been stored in a secure but accessible place?	59
		23) Are repair workers and outside technicians required to adhere to the organization's security policies concerning sensitive information?	59
		Rebuff Theft	60
		24) Has all equipment been labeled in an overt way that clearly and permanently identifies its owner (e.g., the school name)?	60

BEST COPY AVAILABLE

		25) Has all equipment been labeled in a covert way that only authorized staff would know to look for (e.g., inside the cover)?	60
		26) Have steps been taken to make it difficult for unauthorized people to tamper with equipment (e.g., by replacing case screws with Allen-type screws)?	60
		27) Have security staff been provided up-to-date lists of personnel and their respective access authority?	60
		28) Are security staff required to verify identification of unknown people before permitting access to facilities?	60
		29) Are security staff required to maintain a log of all equipment taken in and out of secure areas?	60
		Attend to Portable Equipment and Computers	60
		30) Do users know not to leave laptops and other portable equipment unattended outside of the office?	60
		31) Do users know and follow proper transportation and storage procedures for laptops and other portable equipment?	60
		Regulate Power Supplies	61
		32) Are surge protectors used with all equipment?	61
		33) Are Uninterruptible Power Supplies (UPSs) in place for critical systems?	61
		34) Have power supplies been "insulated" from environmental threats by a professional electrician?	61
		35) Has consideration been given to the use of electrical outlets so as to avoid overloading?	61
		36) Are the negative effects of static electricity minimized through the use of anti-static carpeting, pads, and sprays as necessary?	61
		Protect Output	61
		37) Are photocopiers, fax machines, and scanners kept in open view?	61

BEST COPY AVAILABLE

		38) Are printers assigned to users with similar security clearances?	61
		39) Is every printed copy of confidential information labeled as "confidential"?	62
		40) Are outside delivery services required to adhere to security practices when transporting sensitive information?	62
		41) Are all paper copies of sensitive information shredded before being discarded?	62

CHAPTER 6

Protecting Your System: Information Security

CHAPTER 6 IN A NUTSHELL

Introduction to Information Security pg 67
Commonly Asked Questions pg 67
Policy Issues pg 68
Information Security Countermeasures pg 69
Information Security Checklist pg 74

Introduction to Information Security

As stated throughout this document, one of an organization's most valuable **assets** is its **information.** Local, state, and federal laws require that certain types of information (e.g., individual student records) be protected from unauthorized release (see Appendix B for a FERPA Fact Sheet). This facet of information security is often referred to as protecting confidentiality. While confidentiality is sometimes mandated by law, common sense and good practice suggest that even non-**confidential information** in a **system** should be protected as well—not necessarily from unauthorized release as much as from unauthorized modification and unacceptable influences on its accessibility.

Components of Information Security[20]

Confidentiality:	Preventing unauthorized disclosure and use of information
Integrity:	Preventing unauthorized creation, modification, or deletion of information
Availability:	Preventing unauthorized delay or denial of information

The terms data and information are often used synonymously, but information refers to data that have meaning. For example, "87 percent" is data. It has no meaning by itself until it is reported as a "graduation rate," and then it becomes information.

Commonly Asked Questions

Q. *If an organization maintains physical, software, and user access security, isn't information security addressed by default?*

A. Yes and no. Information **backups** and their storage are surely safer when the building is secure, **software** is used properly, and unauthorized **users** are effectively restricted. However, these security features are meaningless if the information that is being backed up and stored wasn't maintained in a sound way in the first place. While there is no doubt that physical, software, and user **access** security strategies all

contribute to protecting information, ignoring those initiatives that are aimed directly at securing information is not a wise plan.

Q. Isn't there software that can protect my information?

A. Yes, a variety of software products can help your organization in its effort to secure its information and system, but only a thorough, well-conceived, and committed effort to develop and implement an overarching security plan will prove effective in the long run.

Q. *Doesn't it make sense to just go ahead and encrypt all information?*

A. Not necessarily. **Encryption** and **decryption** are time consuming. If information is confidential, then additional time for encrypting and decrypting makes sense. But if the **files** aren't confidential, why would you slow down processing speed for an unnecessary step? And while encryption is a good practice for **sensitive information** or information that is being transmitted over unsecured lines, it should be noted that it is not a complete security strategy in itself. Encrypting information protects files from breaches in confidentiality, but the **risks** of unauthorized or accidental modification (including destruction) and/or denial of use are still real.

While encryption prevents others from reading your information, encrypted files can still be damaged or destroyed so that they are no longer of any use to you.

Policy Issues

Perhaps more than any other aspect of system security, protecting information requires specific procedural and behavioral activities. Information security requires that **data** files be properly created, **labeled**, stored, and backed up. If you consider the number of files that each employee uses, these tasks clearly constitute a significant undertaking. Policy-makers can positively affect this effort by conducting an accurate **risk assessment** (including properly identifying sensitive information maintained in the system). They should also provide organizational support to the security manager as he or she implements and monitors security regulations. The security manager must be given the authority and budget necessary for training staff appropriately and subsequently enforcing information security procedures at all levels of the organizational hierarchy.

Guidelines for security policy development can be found in Chapter 3.

A final consideration for policy-makers is information retention and disposal. All information has a finite life cycle, and policy-makers should make sure that mechanisms are in place to ensure that information that is no longer of use is disposed of properly.

Information Threats (Examples)

As discussed more completely in Chapter 2, a **threat** is any action, actor, or event that contributes to risk. Examples of information threats include:

- Natural events (e.g., lightning strikes, and aging and dirty media)
- Intentional acts of destruction (e.g., hacking and viruses)
- Unintentionally destructive acts (e.g., accidental **downloading** of computer viruses, programming errors, and unwise use of magnetic materials in the office)

As discussed more completely in Chapter 2, a threat is any action, actor, or event that contributes to risk.

Information Security Countermeasures

The following **countermeasures** address information security concerns that could affect your site(s). These strategies are recommended when **risk assessment** identifies or confirms the need to counter potential breaches in your system's information security.

A countermeasure is a step planned and taken in opposition to another act or potential act.

Countermeasures come in a variety of sizes, shapes, and levels of complexity. This document endeavors to describe a range of strategies that are potentially applicable to life in education organizations. In an effort to maintain this focus, those countermeasures that are *unlikely* to be applied in education organizations are *not* included here. If after your risk assessment, for example, your security team determines that your organization requires high-end countermeasures like retinal scanners or voice analyzers, you will need to refer to other security references and perhaps hire a reliable technical consultant.

- Transmit Information Securely (including **e-mail**):
  - *Use e-mail only for routine office communication:* Never send sensitive information as e-mail. If e-mail absolutely must be used, encrypt the file and send it as an attachment rather than in the text of the e-mail message.
  - *Encrypt everything before it leaves your workstation:* Even your **password** needs to be encrypted before leaving the workstation on its way to the **network server**—otherwise it could be intercepted as it travels network connections.
  - *Physically protect your data encryption devices and **keys:*** Store them away from the **computer** but remember where you put them. Use the same common-sense principles of protection you should be giving your bank card's personal identification number (PIN).
  - *Inform staff that all messages sent with or over the organization's computers belong to the organization:* This is a nice way of saying that everything in the office is subject to monitoring.
  - *Use dial-up communication only when necessary:* Do so only after the line has been satisfactorily evaluated for security. Do not publicly list dial-up communication telephone numbers.
  - *Confirm that outside networks from which there are dial-ins satisfy your security requirements:* Install automatic terminal identification, dial-back, and encryption features (technical schemes that protect transmissions to and from **off-site** users).
  - *Verify the receiver's authenticity before sending information anywhere:* Ensure that users on the receiving end are who they represent themselves to be by verifying:
    a. *Something they should know*—a password or encryption key; this is the least expensive measure but also the least secure.
    b. *Something they should have*—for example, an electronic keycard or smart card.

Select only those countermeasures that meet perceived needs as identified during risk assessment and support security policy.

Countermeasures like biometrics are probably beyond the realm of possibility (and necessity) in most, if not all, education organizations.

c. *Something they are*—**biometrics** like fingerprinting, **voice recognition,** and retinal scans; these strategies are more expensive but also more secure.

- *Consider setting up pre-arranged transmission times with regular information trading partners:* If you know to expect transmissions from your trading partners at specific times and suddenly find yourself receiving a message at a different time, you'll know to scrutinize that message more closely. Is it really your trading partner sending the message? Why has the pre-arranged time been ignored? Has the message been intercepted and consequently knocked off schedule?
- *Maintain security when shipping and receiving materials:* When sending sensitive information through the mail, or by messenger or courier, require that all outside service providers meet or exceed your security requirements.

Pre-arranged transmission times set for the middle of the night (e.g., 1:37 a.m.) may seem odd, but they can increase security because there is less traffic on telephone lines and fewer hackers snooping around at such odd hours.

Present Information for Use in a Secure and Protected Way:

- *Practice "views" and "table-design" applications:* A "view" selects only certain fields within a table of information for display, based on the user's access rights. Other table fields are excluded from the user's view and are thus protected from use. For example, although a school record system may contain a range of information about each student, Food Services staff can view only information related to their work and Special Education staff can view only information related to their work. This type of system maintains information much more securely than traditional paper systems, while at the same time increasing statistical utility and accountability options.
- *Use "key identifiers" to link segregated information:* If record information is maintained in a segregated manner (e.g., testing files are kept in a different **database** than special education files) for security purposes, a common file identifier (e.g., a Social Security Number) can be used to match records without unnecessarily divulging the identity of individuals and compromising confidentiality.

Back up Information Appropriately (see Chapter 4):

- *Back up not only information, but also the **programs** you use to access information:* Back up **operating system** utilities so that you retain access to them even if your **hard drive** goes down. Also maintain current copies of critical **application software** and documentation as securely as if they were sensitive data. Caution: Some proprietary software providers may limit an organization's legal right to make copies of programs, but most allow for responsible backup procedures. Check with your software provider.
- *Consider using backup software that includes an encryption option when backing up sensitive information:* Encryption provides additional security that is well worth the extra effort, since it ensures that even if unauthorized users access your backup files, they still can't break confidentiality without also having access to

Many organizations prefer that users *back up only their own data files*—leaving software and operating system backups in the responsible hands of the security manager or system administrator.

your encryption key. If you adopt this recommendation, be sure to change your encryption key regularly.

- *Verify that your backups are written to the **disk** or **tape** accurately:* Choose a backup program that has a verification feature.
- *Rotate backup tapes:* Although backup tapes are usually quite reliable, they tend to lose data over time when under constant use. Retire tapes after two to three months of regular use (i.e., about 60 uses) to a backup activity that requires less regular use (e.g., program backups). Also note that routine tape drive cleaning can result in longer tape life.
- *Maintain a log of all backup dates, locations, and responsible personnel:* Accountability is an excellent motivator for getting things done properly. Remember to store the logs securely.
- *Avoid over-backing up:* Too many backup files can confuse users and thereby increase the possibility of exposing sensitive information. Clear hard drives, servers, and other **storage media** that contain old backup files to save space once you have properly secured (and verified) the last complete and partial backup.
- *Test your backup system:* This point has been made numerous times throughout the document, but it truly cannot be overemphasized!

I'm trying to back up the system, but I can't find the reverse gear on this thing.

Store Information Properly (see Chapter 5):

- *Apply recommended storage principles as found in this document to both original and backup files alike:* Backup files require the same levels of security as do the **master files** (e.g., if the original file is confidential, so is its backup).
- *Clearly label disks, tapes, containers, cabinets, and other storage devices:* Contents and sensitivity should be prominently marked so that there is less chance of mistaken identity.

It Really Happens!

As Principal Brown's secretary, Marsha didn't have time for all the difficulties she was having with her computer—well, it wasn't really her computer that was having problems, but her most important files (and that was worse). Fed up with having to retype so many lost files, she finally called in the vendor who had sold the school all of its equipment. The vendor appeared at her office promptly and asked her to describe the problem.

"Well," Marsha explained, "I keep a copy of all of my important files on a 3½ inch disk, but when I go to use them, the files seem to have disappeared. I know that I'm copying them correctly, so I just can't understand it. I don't know if it's the word processing software or what, but I'm tired of losing all of my important files."

The vendor asked whether it was possible that Marsha was using a bad disk. "I thought about that," she replied as if prepared for the question, "but it has happened with three different disks. It just has to be something else." Marsha reached for a disk that was held to the metal filing cabinet next to her desk by a colorful magnet. "You try it."

"That's a very attractive magnet," the vendor said as Marsha handed over the disk. "Do you always use it to hold up your disks?"

"Yes, it was a souvenir from Dr. Brown's last conference. I just think it's beautiful. Thanks for noticing."

"It is beautiful," the vendor replied, "but you know that it's also the root of all your problems. Every time you expose a disk to that magnet, it erases the files. That's just the way magnets and computer disks get along—like oil and water. Try storing the disk away from the magnet and your troubles, not your files, will soon disappear."

- *Segregate sensitive information:* Never store sensitive information in such a way that it commingles with other data on **floppy disks** or other removable data storage media.
- *Restrict handling of sensitive information to authorized personnel:* Information, programs, and other data should be entered into, or exported from, the system only through acceptable channels and by staff with appropriate clearance.
- **Write-protect** *important* ***files:*** Write-protection limits accidental or malicious modification of files. Note that while write-protection is effective against some viruses, it is by no means adequate virus protection in itself.
- *Communicate clearly and immediately about security concerns:* Train staff to promptly notify the system administrator/security manager when data are, or are suspected of being, lost or damaged.
- *Create a* ***media library*** *if possible:* Storing **backups** and sensitive material in a single location allows for security to be concentrated (and perhaps even intensified). Note, however, that an on-site media library is not a substitute for **off-site** backup protection.

BEST COPY AVAILABLE

- Dispose of Information in a Timely and Thorough Manner:
  - *Institute a specific information retention and disposal policy as determined by the organization's needs and legal requirements:* All data have a finite life cycle. Consult local, federal, and state regulations for guidance before implementing the following:
    - Establish a realistic retention policy.
    - Mark files to indicate the contents, their expected life cycle, and appropriate destruction dates.
    - Do not simply erase or reformat media, but overwrite it with random binary code. Sophisticated users can still access information even after it has been erased or reformatted, whereas overwriting actually replaces the discarded information.
    - Consider **degaussing** (a technique to erase information on a magnetic media by introducing it to a stronger magnetic field) as an erasure option.
    - Burn, shred, or otherwise physically destroy storage media (e.g., paper) that cannot be effectively overwritten or degaussed.
  - *Clean tapes, disks, and hard drives that have stored sensitive data before reassigning them:* Never share disks that have held sensitive data unless they have been properly cleaned. Also remember to clean magnetic storage media before returning it to a vendor for trade-ins or disposal.

Retaining data beyond its useful life exposes the organization to unnecessary risk.[21]

Even if a vendor replaces a hard drive, require that the old one be returned so that you can verify that it has been cleaned and disposed of properly.

It Really Happens!

Trent couldn't believe his eyes. Displayed before him on a monitor in the high school computer lab were the grades of every student in Mr. Russo's sophomore English classes:

Student Name	Grades	Comments
Linda Foster	C-, C, C+, C	Improving slightly, but unable to make sufficient gains; a candidate for learning disability testing?

All Trent had done was hit the "undelete" function in the word processing software to correct a saving mistake he had made, and suddenly a hard drive full of Mr. Russo's files were there for the taking. Luckily for Mr. Russo, his sophomores, and the school, Trent realized that something was very wrong. He asked the lab supervisor, Ms. Jackson, where the computers had come from.

"Most of them have been recycled," she admitted. "Teachers and administrators were given upgrades this year, so their old machines were put to good use in the labs. They should still be powerful enough to handle your word processing. Why?"

Trent showed Ms. Jackson what he had uncovered about the sophomore English students. She gasped, "Oh my goodness, they gave us all these computers without clearing the hard drives properly. I bet it's that way across the district. Trent, you may have just saved us from a potentially disastrous situation. That information is private and certainly shouldn't be sitting here for anyone in the computer lab to see. I've got some phone calls to make!"

Information Security Checklist

While it may be tempting to refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement **security policy** throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 6

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points for Information Security	Page
		Transmit Information Securely (including e-mail)	69
		1) Is e-mail used for only the most routine of non-sensitive office communication?	69
		2) Is everything, including passwords, encrypted before leaving user workstations?	69
		3) Are encryption keys properly secured?	69
		4) Has staff been informed that all activity on the organization's equipment belongs to the organization and is subject to monitoring?	69
		5) Is dial-up communication avoided as much as is possible?	69
		6) Are outside networks required to meet your security expectations?	69
		7) Is the identity of information recipients verified before transmission?	69
		8) Have times for information transmission been pre-arranged with regular trading partners?	70
		9) Are security issues considered before shipping sensitive materials?	70

BEST COPY AVAILABLE

		Present Information for Use in a Secure and Protected Way	**70**
		10) Are "views" and "table-design" applications being practiced?	**70**
		11) Are "key identifiers" used when linking segregated records?	**70**
		Backup Information Appropriately	**70**
		12) Are programs that are used to access information backed up?	**70**
		13) Does backup software include an encryption option that is used?	**70**
		14) Does backup software include a verification feature that is used?	**71**
		15) Are backup tapes retired after a reasonable amount of use?	**71**
		16) Is a log of all backup dates, locations, and responsible personnel kept and maintained securely?	**71**
		17) Is an effort made to avoid "over-backing up" (i.e., are old backups removed to avoid "clutter")?	**71**
		18) Does the backup system pass regularly administered tests of its effectiveness?	**71**
		Store Information Properly	**71**
		19) Are recommended storage principles applied to master files and their backups alike?	**71**
		20) Are disks, tapes, containers, cabinets, and other storage devices clearly labeled?	**71**
		21) Is sensitive information segregated (i.e., is it maintained separately from normal use information at all times)?	**72**
		22) Is the handling of sensitive information restricted to authorized personnel?	**72**

		23) Are important files write-protected?	72
		24) Does staff know to communicate security concerns immediately?	72
		25) Has a secure media library been created as is possible?	72
		Dispose of Information in a Timely and Thorough Manner	73
		26) Has an information retention and disposal policy been implemented ?	73
		27) Are magnetic media that contain sensitive information properly cleaned before reuse or disposal?	73

There is no record in history of a nation that ever gained anything valuable by being unable to defend itself.

—H.L. Mencken

BEST COPY AVAILABLE

CHAPTER 7

Protecting Your System: Software Security

CHAPTER 7 IN A NUTSHELL:

Introduction to Software Security pg 77
Commonly Asked Questions pg 77
Policy Issues pg 78
Software Security Countermeasures pg 78
Software Security Checklist pg 83

Introduction to Software Security

Saying that **software** is an integral part of your **computer** system is like saying that the steering wheel is an integral part of an automobile. It's an understatement if ever there was one. All the technological and mechanical muscle in the world is virtually useless without a way of controlling it—and software is precisely the means by which **users** control what they are doing on a computer **system. Application software** affects all areas of computing. It defines the concepts of word processing and spreadsheets, and allows for **e-mail** and other forms of electronic communication that have recently become so prevalent. Its security, therefore, is essential to the overall security of your information and system.

Commonly Asked Questions

Q. ***Doesn't software come with its own security?***

A. At some level, the answer is yes. Many types of software include security components within their programming, but, generally speaking, these safeguards are of a fairly simple nature. In most cases, they can be circumvented easily by skilled intruders. Effective software security requires a host of well-conceived policies aimed at software procurement, development, and use that must be realized through staff activity and organizational commitment.

Q. ***Isn't software security starting to get too technical for policy-makers?***

A. Not necessarily. Effective software security can demand technical knowledge and experience, but policy-makers can overcome these concerns by including **technical support staff** in the policy development process.

Q. ***How can an organization overcome programming errors and viruses?***

A. Any new or modified software has the potential to have programming errors. In fact, errors are a normal part of the product refinement process. **Viruses,** while not a normal part of any healthy process, have also become far from uncommon. But a rigorous pre-implementation testing routine (developed in coordination with technical staff) can diagnose these problems before they damage the organization's system or **information.** It is imperative that such testing be done on dedicated computers that are not connected to the organization's **network** and with dummy **data** in order to minimize **risk.**

Policy Issues

Because certain aspects of software security can become quite technical, administrators should work closely with technical staff throughout the policy-development process.

Because certain aspects of software security can become quite technical, administrators should work closely with technical staff throughout the policy-development process. Software security requires policies on software management, acquisition and development, and pre-implementation training. Unlike many personnel aspects of system security, appropriate software use requires that products and equipment match in a range of technical specifications. Policy-makers may, therefore, choose to pay close attention to the advice of technical staff when considering software issues and generating policy. Software users (virtually anyone who turns on a computer) should also be surveyed about the types of software required to perform their jobs, the ways in which those pieces of software are used, and the kinds and amount of training that are necessary to properly prepare staff to meet their job requirements.

Software Threats (Examples)

Examples of software **threats** include:

- Natural events (e.g., aging and dirty media)
- Intentional acts of destruction (e.g., hacking, creation of computer viruses, and copyright infringement)
- Unintentionally destructive acts (e.g., accidental **downloading** of computer viruses, losing instructions, and programming errors)

As discussed more completely in Chapter 2, a threat is any action, actor, or event that contributes to risk.

Software Security Countermeasures

A countermeasure is a step planned and taken in opposition to another act or potential act.

The following **countermeasures** address software security concerns that could affect your site(s). These strategies are recommended when **risk assessment** identifies or confirms the need to counter potential breaches in the security of your software system.

Countermeasures come in a variety of sizes, shapes, and levels of complexity. This document endeavors to describe a range of strategies that are potentially applicable to life in education organizations. To maintain this focus, those countermeasures that are *unlikely* to be applied in education organizations are *not* included here. If after your risk assessment, for example, your security team determines that your organization requires high-end

countermeasures like retinal scanners or voice analyzers, you will need to refer to other security references and perhaps hire a technical consultant.

- Coordinate (and Centralize) the Organization's Software Management:
  - *Centrally control all* ***critical system*** *software:* (1) Know what **programs** are being added, deleted, and changed in your system; (2) control all additions, deletions, and modifications; and (3) take all necessary steps to ensure that new and old software work together appropriately (i.e., that they **interface**).
  - *Initiate formal testing and certification procedures for new/modified software:* Require that any new or modified software be tested rigorously and certified as fully operational before releasing it for general use.
  - *Maintain an* ***off-site*** *location for critical backup copies (see Chapter 6):* **Backups** of any and all software, **databases,** and information that serve critical **functions** should reside in a secure off-site location and be readily accessible when and if needed. Backups require the same level of protection as **master files** (i.e., if the **files** are designated as **confidential,** treat the backups as confidential as well). Periodically check that the backups function as expected so that there are no surprises if and when they are really needed.
  - *Secure master copies of software and associated documentation:* If master copies and/or their instructions are lost, an entire system can be put in jeopardy. But while documentation must be protected, it must also be kept available to users who have legitimate questions about proper use of the software.
  - *Never lend or give proprietary software to unlicensed users:* By definition, proprietary software means that it isn't yours to give—someone else makes their living by selling it.

Select only those countermeasures that meet perceived needs as identified during the risk assessment and that support security policy.

Test backup files periodically to ensure that they "restore" properly.

It Really Happens!

Every state education agency has its computer whiz—that person who not only can program in seven different languages, but can also fix everyone else's system whenever and whatever problems arise. Martin was his agency's sensation. He was a programmer by training, but had so mastered system technology that it was eventually understood that he should be "doing his own thing." He was always working on some kind of new program or another that would inevitably revolutionize the way the state managed its data. Whenever there was need for a special computer job, there was little question where folks could turn.

But one afternoon Martin and the state superintendent found out that even the computer genius wasn't perfect. It seems that Martin's hard drive had crashed that morning as he was putting the finishing touches on a project that was needed by his boss that very day. Martin's initial response was to tell the superintendent not to panic, "Don't worry, I'm not foolish enough to go to all this effort and not back up my work files." But when Martin tried to access the backup files on another computer, he got nothing but error messages. It was then that he remembered that the files had all been created with the new software he had purchased especially for the superintendent's project. He also remembered that since he was the only one using the software, he hadn't loaded it on to anyone else's machine but his own.

Now panicked himself, Martin looked feverishly for the software's master diskettes. He checked the stacks of stray disks and piles of loose paper that littered his office. He went through every hanging folder in his filing cabinet. Where could those disks be? In a last ditch effort, he even called the local computer store to see if they could help. They politely told him that he'd have to repurchase the software unless he could produce a valid user license number—which could be found on the packaging of the master diskettes. That wasn't any help.

In the end, Martin didn't get the project to the superintendent on time. He eventually found the master diskettes at his home (where he had taken all of the documentation to read one night several weeks earlier). But because he had been accessing the electronic HELP file through the software as soon as it had been loaded onto his computer, he had never again thought about the paper documentation or the master diskettes. It was a tough lesson to learn—and it cost him some of the confidence he had worked so hard to earn from his boss.

- *Tolerate nothing but licensed and organizationally approved software on workplace equipment:* Games are fun and software from home can sometimes be useful, but they have no place on organizational equipment unless explicitly authorized.
- *Monitor **software** use (and **hard drive** inventories) to counter possible copyright infringements:* Unlicensed software on organizational equipment puts the entire organization at risk for fines and other penalties stemming from copyright violations. Software inventories should include the name of the manufacturer, **version** number, assigned computer (as applicable), and function.
- *Permit only authorized personnel to install software:* In this way you know exactly what software is being introduced to your system and that it is being installed properly.
- *Train staff on software use and security policies:* The best designed software for **accessing** and manipulating information is useless if staff are unable to use it properly.

Software acquisition and development is addressed in greater detail in another National Center for Education Statistics publication, *Technology @ Your Fingertips* (see Appendix C).

Regulate Software Acquisition and Development:[11]

- *Define security needs before purchasing or developing new software:* After identifying your needs through a risk assessment (see Chapter 2), the findings should be used as the criteria by which you select appropriate software products.
- *Require written authorization before anyone tampers with software:* Any changes to software requires a paper trail of what, why, and under whose auspices software was modified.
- *Conduct design reviews throughout the development process:* Continued feedback from expected users during development ensures that the product will satisfy **functional specifications** and security requirements.
- *Modify archived copies of software (not the copy that is up and running on the system):* By doing so, you can be sure that you are not putting active applications and files at risk. Once the modified copy passes testing and is certified as operational, then and only then should it be loaded onto the system for use with "live" data.

- *Require that all software developed or modified by a* ***programmer*** *be reviewed by a second, independent programmer:* This review should verify that all **code** is appropriate and correct.
- *Maintain master files of all developed software independent of the programmer:* Software belongs to the organization, not the programmer. By controlling all original copies, the organization clearly guarantees this ownership.
- *Require documentation for all new or revised* ***programming:*** Requisite documentation includes the name of the developer, the name of the programming language, the development date, the revision number, and the location of the master copy (i.e., the source code).
- *Verify authenticity of public programs:* If software downloaded from the **Internet** must be used with **sensitive information**,

It Really Happens!

The management team had finally had enough of Lou the programmer. They might have been able to overlook his daily late arrivals and early departures (rumor had that even the airlines kept to their schedules better than Lou), but when he started his own computer consulting business on district time, they'd had enough. As his direct supervisor, Charlotte accepted the responsibility of informing Lou that he was being dismissed.

Charlotte and the Director of Personnel called Lou to the conference room to break the news. "Lou," Charlotte began, "you recall that six months ago the three of us met to discuss your work patterns. We informed you that they were unsatisfactory and that things would need to change. At that time you agreed to try to improve your performance. Unfortunately, it has become clear through this whole business of you leaving work during office hours to attend to your personal consulting that your performance has not improved. Therefore, I must inform you that your contract is being terminated."

Lou paused to assimilate Charlotte's message. "You mean that you're firing me?"

"Yes," Charlotte replied, "you are being terminated."

"Nah," Lou protested, "you don't want to do that."

Charlotte was surprised by his audacity, "Yes, we do."

"No," Lou clarified, "I mean you really don't want to do that. I've been working on the programming for the School Report Cards for the last six months. You need it if you are to have any chance of getting them out this year. It really would be a mistake to get rid of me at this point."

"Are you threatening to withhold work that we've already paid you for?" the Director of Personnel interjected.

Lou sensed the trap. "No, not at all. I'd never do that. But I can tell you that I've had a tough time keeping things organized on my hard drive, so I've had to store a lot of my programs on diskettes. Suddenly I'm having difficulty remembering where I've put them all. And if I'm having problems figuring it all out, I seriously doubt that you'd ever be able to find those files if you hired someone to replace me."

While the vast majority of staff are probably completely **trustworthy, they** are not impervious to accidents or other events that could keep them from showing up for work some day. The organization is entitled to, and should, keep updated copies of everyone's work files.

Charlotte paraphrased the effective, if thinly veiled, threat. "So, you're saying that we have a choice between keeping you or saying goodbye to the School Report Cards?"

Lou smiled smugly, "You said it, not me... but I like the way you think. Now, maybe it's time that we talk about a raise."

be sure that it has not been tampered with by checking for a **digital signature** to verify its authenticity.

Because new products are bound to have their share of kinks, software's "cutting edge" is often referred to only half-jokingly as its "bleeding edge." Bleeding edge software should be avoided for mission-critical activities.

- Thoroughly Test Newly Acquired and Developed Software:
  - *Specifically search for common types of computer viruses:* Have technical staff check for common viruses such as **Trojan Horses** and **worms.**
  - *Verify that all software **user functions** are working properly before putting the **software** into operation:* Check that new software meets anticipated user needs, current system requirements, and all organizational security standards. This recommendation is also applicable when **upgrading** software.
  - *Back up old files before installing new software and software upgrades:* Don't risk the latest copies of your files/records until you're certain that your new versions are up and running properly.
  - *Never test application software with "live" data:* Don't risk losing real information if the software doesn't pass the test. Instead, verify software integrity with dummy files and/or copies of non-sensitive files.
  - *Test on independent machines:* Initial software testing should never occur on computers that are connected to the system. By maintaining a separate test environment, the entire system is not at risk if the software malfunctions.
  - *Run existing and upgraded versions of software in parallel during final testing phases:* By running the old software at the same time as the new and improved software, you can verify that the new versions generate the same or better results than the existing system.

Avoid the "ohnosecond"—that fraction of a second in which computer users realize that they have just made a huge mistake with their data.

—adapted from *The Electronic Traveller*
by Elizabeth P. Crowe

Software Security Checklist

While it may be tempting to simply refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement **security policy** within and throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 7

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points for Software Security	Page
		Coordinate (and Centralize) Software Management	79
		1) Is critical system software controlled by central administration?	79
		2) Has a formal testing and certification procedure for new/modified software been developed and initiated?	79
		3) Are backups of critical software and information maintained in secure facilities at an off-site location?	79
		4) Have all master copies of software been properly secured?	79
		5) Has all software documentation been secured appropriately?	79
		6) Does the organization expressly forbid lending or giving proprietary software to unlicensed users?	79
		7) Does workplace equipment store and use only licensed and organizationally-approved software?	80
		8) Are software use and hard drive inventories monitored for copyright violations?	80
		9) Is installation of software limited to authorized personnel?	80
		10) Are staff adequately trained in software use and security?	80

BEST COPY AVAILABLE

		Regulate Software Acquisition and Development	**80**
		11) Are risk assessment findings considered before purchasing and developing new software?	**80**
		12) Is written authorization required before any software is modified?	**80**
		13) Is software design reviewed throughout the development process?	**80**
		14) Are active applications and files (i.e., those actively running on the system) properly shielded from experimental/developmental software?	**80**
		15) Is all software that is created or modified by a programmer subjected to review by a second programmer?	**81**
		16) Are all master copies of internally developed software maintained by the organization and not the programmer?	**81**
		17) Is suitable documentation prepared for all newly developed software?	**81**
		18) Has all public software accessed via the Internet been verified for authenticity?	**81**
		Thoroughly Test Newly Acquired and Developed Software	**82**
		19) Are common types of viruses searched for specifically during new software testing?	**82**
		20) Have all user functions been verified before new software is put into operation?	**82**
		21) Are all files backed up before installing and upgrading software?	**82**
		22) Are "live" data protected from new application testing?	**82**
		23) Is new application testing done on non-networked computers?	**82**
		24) Has old and new software been run in parallel to compare results?	**82**

BEST COPY AVAILABLE

CHAPTER 8

Protecting Your System: User Access Security

CHAPTER 8 IN A NUTSHELL:

Introduction to User Access Security	pg 85
Commonly Asked Questions	pg 86
Policy Issues	pg 87
User Access Security Countermeasures	pg 87
User Access Security Checklist	pg 92

Introduction to User Access Security

User access security refers to the collective procedures by which authorized users **access** a **computer** system and unauthorized users are kept from doing so. To make this distinction a little more realistic, however, understand that user access security limits even authorized users to those parts of the **system** that they are explicitly permitted to use (which, in turn, is based on their "**need-to-know**"). After all, there is no reason for someone in Staff Payroll to be given clearance to **confidential** student records.

A person with a "need-to-know" has been designated by school officials as having a legitimate educational or professional interest in accessing a record.

It Really Happens!

Kim approached Fred cautiously. As the security manager, she knew how important it was to gather information completely before jumping to conclusions. "Fred, my review of our computer logs shows that you have been logging in and looking at confidential student information. I couldn't understand why someone in Food Services would need to be browsing through individual student test scores, so I thought I'd come by and ask you."

Fred looked up at Kim as he if was surprised to be entertaining such a question. "Are you forgetting that I'm authorized to access student records?"

"You're authorized to access specific elements that relate to a student's free- and reduced-price lunch eligibility," Kim clarified. "That's the limit of your need-to-know."

"I didn't know that my access was limited," Fred asserted honestly. "I figured that if my password got me into a file, it was fair game."

Kim paused, realizing that it might be reasonable for Fred to have assumed that he was allowed to read a file if his password gave him access. "Hmm, I see your point, Fred, but in truth you shouldn't be accessing student record information that isn't related to your legitimate educational duties. I'm not going to make a big deal of it this time, but from now on, limit your browsing to the free- and reduced-price lunch information. In the meantime, I'm going to send a memo out to staff reminding them what need-to-know really means."

"And you might want to reconsider how our password system works," Fred added. "It would have been very clear to me that I had no business in a file if my password wouldn't get me in."

BEST COPY AVAILABLE

An organization cannot monitor user activity unless that user grants implicit or explicit permission to do so!

While there is no question that an organization has the right to protect its computing and **information resources** through user access security activities, users (whether authorized or not) have rights as well. Reasonable efforts must be made to inform all users, even uninvited **hackers,** that the system is being monitored and that unauthorized activity will be punished and/or prosecuted as deemed appropriate. If such an effort is not made, the organization may actually be invading the privacy rights of its intruders!

An excellent way of properly informing users of monitoring activities is through the opening screen that is presented to them. By reading a warning like the one that follows, users explicitly accept both the conditions of monitoring and punishment when they proceed to the next screen. Thus, the first screen any user sees when **logging into** a secure computer system should be something to the following effect:

Never include the word "Welcome" as a part of the log-in process—it can be argued that it implies that whoever is reading the word is, by definition, *invited* to access the system.

```
WARNING!

This is a restricted network. Use of this network, its
equipment, and resources is monitored at all times
and requires explicit permission from the network
administrator. If you do not have this permission in
writing, you are violating the regulations of this
network and can and will be prosecuted to the full
extent of the law. By continuing into this system, you
are acknowledging that you are aware of and agree
to these terms.
```

Commonly Asked Questions

Q. ***Is it possible to have a secure system if you have employees who telecommute or work otherwise non-traditional schedules?***

A. Yes. While particular **countermeasures** might need to be adjusted to accommodate non-traditional schedules (e.g., the practice of limiting users to acceptable log-in times and locations), a system with **telecommuters,** frequent travelers, and other **remote access** users can still be secure. Doing so may require policy-makers to think more creatively, but each security guideline needs to be customized to meet the organization's needs anyway (see Chapter 2).

Q. ***Is the use of passwords an effective strategy for securing a system?***

A. Just because **password** systems are the most prevalent **authentication** strategy currently being practiced doesn't mean that they have become any less effective. In fact, the reason for their popularity is precisely because they can be so useful in restricting system access. The major concern about password systems is not their technical integrity, but the degree to which (like many strategies) they rely upon proper implementation by users. While there are certainly more expensive and even effective ways of restricting user access, if **risk** analysis determines that a password system meets organizational needs and is most cost-effective, you can feel confident about password protection as long as users

are implementing the system properly—which, in turn, demands appropriate staff training (see Chapter 10).

Q. ***Are all of these precautions necessary if an organization trusts its staff?***

A. Absolutely. While the vast majority of system users are probably trustworthy, it doesn't mean that they're above having occasional computing accidents. After all, most system problems are the result of human mistake. By instituting security procedures, the organization protects not only the system and its information, but also each user who could at some point unintentionally damage a valued **file.** By knowing that "their" information is maintained in a secure fashion, employees will feel more comfortable and confident about their computing activities.

Trust just simply is not an acceptable security strategy.

Initiating security procedures also benefits users by:

1) Helping them to protect their own files

2) Decreasing the likelihood of their improperly releasing confidential information

3) Educating them about what is and is not considered to be appropriate behavior

Policy Issues

User access security demands that all persons (or systems) who engage **network** resources be required to identify themselves and prove that they are, in fact, who they claim to be. Users are subsequently limited to access to those files that they absolutely need to meet their job requirements, and no more. To accomplish this, decision-makers must establish policies regulating user account systems, user authentication practices, log-in procedures, physical security requirements, and remote access mechanisms.

Guidelines for security policy development can be found in Chapter 3.

User Access Threats (Examples)

Examples of user access **threats** include:

- Intentional acts (e.g., shared user accounts, hacking, and user **spoofing** or impersonating)
- Unintentional acts (e.g., delayed termination of inactive accounts, unprotected passwords, and mismanaged remote access equipment)

As discussed more completely in Chapter 2, a threat is any action, actor, or event that contributes to risk.

User Access Security Countermeasures

The following countermeasures address user access security concerns that could affect your site(s) and equipment. These strategies are

recommended when **risk assessment** identifies or confirms the need to counter potential user access breaches in your security system.

Countermeasures come in a variety of sizes, shapes, and levels of complexity. This document endeavors to describe a range of strategies that are potentially applicable to life in education organizations. In an effort to maintain this focus, those countermeasures that are *unlikely* to be applied in education organizations are *not* included here. If after your risk assessment, for example, your security team determines that your organization requires high-end countermeasures like retinal scanners or voice analyzers, you will need to refer to other security references and perhaps hire a reliable technical consultant.

Select only those countermeasures that meet perceived needs as identified during risk assessment (Chapter 2) or support policy (Chapter 3).

- Implement a Program in Which Every User Accesses the System by Means of an Individual Account:
  - *Limit user access to only those files they need to do their jobs:* Providing access that is not needed greatly contributes to risk without a corresponding increase in benefit. Why bother?
  - *Avoid shared accounts:* Individual activity cannot be differentiated unless there are individual accounts.
  - *Secure the user account name list:* Because of its importance to system security, the user account list should be considered to be confidential and should never be made public. Give strong consideration to storing it as an **encrypted** file.
  - *Monitor account activities:* Keep a record of all system use (many systems perform this function through an **audit trail** feature).
  - *Terminate dormant accounts after a pre-set period of inactivity (e.g., 30 days):* Legitimate users can always reapply and reestablish their accounts.

See Chapter 9 for guidelines for authenticating messages transmitted over outside networks.

- Require Users to "Authenticate" Themselves in Order to Access Their Accounts (i.e., make sure that they prove that they are who they are representing themselves to be):
  - *Select an authentication system:* The right choice for an authentication system depends on the needs of the organization and its system, and should be based on the findings of a risk assessment (see Chapter 2). Note that the following options progress from least secure to most secure, as well as (not surprisingly), least expensive to most expensive:
    1) Something the user knows (e.g., a password—see below)
    2) Something the user has (e.g., an electronic key card)
    3) Something the user is (e.g., **biometrics**—finger printing, **voice recognition,** and hand geometry)

Countermeasures like biometrics are probably beyond the realm of possibility (and necessity) in most, if not all, education organizations.

Passwords

Because passwords are the most common method of user authentication, they deserve special attention.

Password selection:

- Require that passwords be at least six characters in length (although eight to ten are preferable).
- Prohibit the use of passwords that are words, names, dates, or other commonly expected formats.
- Forbid the use of passwords that reflect or identify the account owner (e.g., no birthdates, initials, or names of pets).
- Require a mix of characters (i.e., letters/numbers and upper/lower case if the system is case sensitive).

One way to effectively create apparently random passwords that can be memorized easily is to use the first letter of each word in a favorite quote, capitalize every other letter, and add a number. For example, Longfellow's "One if by land, two if by sea" (from Paul Revere's Ride*) becomes the password "olbLtlbS3".*[21]

Password maintenance:

- Require the system administrator to change all pre-set passwords that are built into **software** (e.g., supervisor, demo, and root).
- Systematically require passwords to be changed at pre-set intervals (e.g., once per month).
- Maintain zero-tolerance for password sharing.
- Forbid unsecured storage of personal passwords (e.g., they should not be written on a Post-It™ note and taped to the side of a **monitor**).
- Never send a password as a part of an **e-mail** message.
- Warn users not to type their password when someone may be watching.
- Mask (or otherwise obscure) password display on the monitor when users type it in.
- Remind users that it is easy to change passwords if they think that theirs may have been compromised.
- Maintain an encrypted history of passwords to make sure that users are not simply recycling old passwords when they should be changing them.
- Monitor the workplace to ensure that all regulations are being followed.

There are tradeoffs associated with making passwords more difficult to remember than a pet's name or a person's initials (e.g., staff are more likely to *write down* password reminders). The costs and benefits of these tradeoffs should be considered in the organization's risk assessment (see Chapter 2).

A Security Manager's Nightmare

"Is our password still 'Fido'?"

It Really Happens!

Principal Mullins was a stickler for rules, but he was also serious about getting the job done. When, two weeks after school had already begun, he learned that none of his three new teachers had yet received accounts on the computer network from central office, he was incensed. They had enough to worry about without being hampered by being kept off-line. He called in his assistant, "I don't care whether security policy prohibits password sharing or not, these people need to get on the system. Let them use my password to log on—it's 'A4a6dc', got that? Make sure that they have access to everything they need to do their jobs!"

The security manager must be open to the concerns of system users. Security is a two-way street on which both users and security personnel have legitimate needs.

Three weeks passed before the system administrator e-mailed Principal Mullins about apparent misuse of his password: "System logs show almost daily incidents when more than one person at a time is trying to log on to the system with your password. Please change the password immediately and let me know if you have any idea about who is misusing it."

Principal Mullins knew that he had not only been risking trouble with the system administrator but also truly jeopardizing system security. Despite his initial (and legitimate) anger about his teachers being unable to access the system, he did not feel good about circumventing agreed-upon policy. Unfortunately, when central office was so unresponsive to the needs of his teachers and school, he felt that he had been left with very few options. He replied to the system administrator: "My three new teachers are using the password since they have yet to be assigned their own network accounts. We are not looking to break good rules, only to do our jobs—please allow us to do so. Find a way to get new staff access to the system in a timely manner and we will surely respect and abide by security policy." Principal Mullins could only hope that the system administrator would understand his position, and that system security had not been violated.

Remember to customize countermeasures to meet organizational and user needs.

Some intruders employ "password dictionaries" that, quite literally, try to match passwords one word at a time for thousands and thousands of attempts!

- Establish Standard Account and Authentication Procedures (known as log-in procedures):
  - *Limit users to acceptable log-in times:* There is no reason for an average day-shift employee to be able to access the system in the middle of the night.
  - *Limit users to acceptable log-in locations:* There is no reason for an average employee with a terminal on his or her desk to access the system from his or her supervisor's desk.
  - *Set reasonable limits to the number of allowable log-in attempts:* Enable the system to assume that anyone who can't enter a password correctly after three attempts may, in fact, not be who they say they are. Allow users more than one or two attempts or else they might make mistakes simply because they are worried about getting shut out. After three incorrect attempts, the account should be suspended (to prevent an intruder from simply calling back and trying three more times). Legitimate users can always have their accounts reopened by contacting the security manager.
  - *Require staff to log off the system and turn off the computer:* The last important step of logging on properly is logging off properly. Users should be required to log off every time they leave their workstations (e.g., for lunch, breaks, and meetings). After all, an unauthorized user has free reign to an authorized user's access when a computer is left unattended and logged into the system.

- Recognize that Routine Physical Security Plays an Important Role in User Access Management (see also Chapter 5):
  - *Protect every access **node** in the system:* An "access node" is a point on a network through which you can access the system. If even one such point is left unsecured, then the entire system is at risk. A good example of frequently forgotten access nodes are modular network plugs that are often built into conference rooms (into which portable computers can be plugged). If unauthorized users can get to such a node with a **laptop,** they are in position to **attack** the system.
  - *Protect cables and wires as if they were access nodes:* If a sophisticated intruder can access a span of **cable** that is used as a connector between pieces of equipment, he or she may be able to access the entire system. Physically accessing the wiring is referred to as "tapping the line." High-end equipment can monitor electrical emanations (known as Radio Frequency Interference) from wiring without even physically touching the cable.
  - *Disconnect floppy drives from **servers:*** A sophisticated intruder can boot-up (the technical term for "starting the system") from an external **disk drive.**
  - *Install **screen savers** (with mandatory locking features):* Prevent information from being read by anyone who happens to be walking past the display monitor.

- Pay Particular Attention to Remote Access Systems (i.e., when someone, including an authorized user, accesses your system from **off-site** via a **modem**):
  - *Consider requiring pre-approval for remote access privileges:* An identified subset of employees to monitor is more manageable than every random person who calls into the system.
  - *Remind staff that remote access is particularly subject to monitoring activities:* Increased risk requires increased vigilance.
  - *Set modems to answer only after several rings:* An authorized user will know that he has dialed a "slow" modem and will therefore be willing to wait. A random-dialer looking to bump into modems may be less likely to be so patient.
  - *Use a "call back" communication strategy with remote access users:* Once users call in and properly identify themselves, the connection is dropped and the system then calls back the authorized users at a pre-approved access location.
  - *Use software that requires "message authentication" in addition to "user authentication":* Even if a user can provide the right password, each message sent and received must have its delivery verified to ensure that an unauthorized user didn't interrupt the transmission.
  - *Never transmit **sensitive information** over public telephone lines unless the transmission has first been encrypted:* Unless a line can be verified as secure, it must be considered to be susceptible to tampering.

See Chapter 9 for more information about securing connections to outside networks, including the Internet.

BEST COPY AVAILABLE

- *Investigate security features of external networks to which the system connects:* The **Internet** and other networks are not just things your staff can access and browse—they are two-way lines of communication. If security cannot be verified, then additional precautions must be taken (e.g., **gateways** and **firewalls**).
- *Install firewalls on your system at external access points:* A firewall is by far the most common way to secure the connection between your network and outside networks. It works by allowing only trusted (authenticated) messages to pass into your internal network from the outside (see also Chapter 9).

School officials allow the use of calculators in the classroom without necessarily understanding how the transistors process mathematical calculations. So, too, can they make informed decisions about highly technical security options like firewalls without having to become experts on installing and operating associated software and hardware.

- *Never list dial-in communication numbers publicly:* Why advertise what authorized users should already know?
- *Disable modems when not in use:* No need to provide a viable line of access to and from the system unless it's necessary.
- *Never leave a modem on automatic answer mode:* Such a practice opens the door to unauthorized and unsupervised system access.
- *Permit modem use only from secure locations:* Never allow a modem to be connected to a system machine that is not itself protected by a firewall or gateway.
- *Grant Internet access only to those employees who need it to perform their jobs:* A student might need the Internet for legitimate learning purposes, but a staff assistant probably does not.
- *Remind students and staff that the Internet (and all system activity for that matter) is for approved use only:* There are countless Internet sites and activities that have no positive influence on the education environment. They have no place on the system.
- *Require all users to sign **Appropriate Use Agreements** before receiving access to the system:* Signed Security Agreements (see Chapter 3) verify that users have been informed of their responsibilities and understand that they will be held accountable for their actions.

User Access Security Checklist

While it may be tempting to refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement **security policy** throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 8

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points for User Access Security	Page
		Design an Appropriate Opening Screen That Users Must Visit Before Accessing the System	86
		1) Is the opening screen clear and specific about the organization's expectations of the user?	86
		2) Does the opening screen require the user to accept the conditions of monitoring and punishment before proceeding?	86
		Implement a User Account System	88
		3) Is file access limited to that information users need to do their jobs?	88
		4) Are shared accounts explicitly prohibited?	88
		5) Is the list of user accounts and names maintained securely?	88
		6) Is account activity properly monitored?	88
		7) Are dormant accounts terminated after pre-set periods of inactivity?	88
		Require Users to Authenticate Themselves	88
		8) Has an appropriate authentication system been selected based on risk assessment findings?	88
		9) Are passwords required to be at least six characters in length?	89
		10) Are names, dates, and other commonly anticipated password formats disallowed?	89
		11) Are passwords that reflect or identify the user forbidden (e.g., initials and pet names)?	89

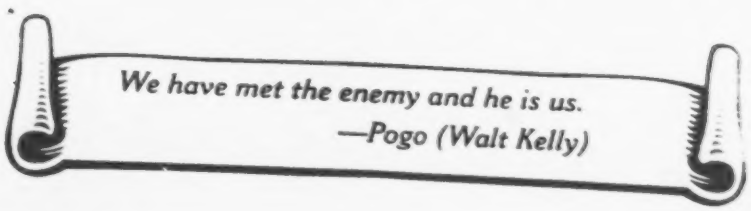
BEST COPY AVAILABLE

		12) Is a mix of letters and numbers, and upper and lower cases required?	89
		13) Is the use of non-words and random characters encouraged	89
		14) Has the system administrator changed all pre-set and packaged passwords?	89
		15) Are passwords required to be changed at regular intervals?	89
		16) Is password sharing expressly forbidden?	89
		17) Are password reminders stored securely by personnel?	89
		18) Have users been warned to never send their password as a part of an e-mail message?	89
		19) Have users been warned not to type in their passwords when someone may be watching?	89
		20) Are password characters masked on display screens?	89
		21) Have users been told that they can, and should, change their password if they think it might be compromised?	89
		22) Is a history of user passwords maintained securely and reviewed routinely to ensure that users are not recycling passwords?	89
		23) Is the workplace appropriately monitored for adherence to security regulations?	89
		Establish Standard Log-in Procedures	90
		24) Is each user limited to acceptable times for logging into the system?	90
		25) Is each user limited to acceptable places for logging into the system?	90
		26) Is there a limit to the number of times a user can attempt to log in incorrectly?	90

BEST COPY AVAILABLE

		27) Do staff know to log off and turn off computers?	90
		Recognize the Importance of Physical Security	91
		28) Have all system access points (nodes) been secured?	91
		29) Has all cabling and wiring been secured?	91
		30) Have floppy drives been disconnected from servers?	91
		31) Are lockable screen savers installed and in use?	91
		Pay Attention to Remote Access (and Modem Use)	91
		32) Is pre-approval required for remote access capabilities	91
		33) Are staff aware that remote access is monitored? Is it?	91
		34) Are modems set to answer only after several rings?	91
		35) Is a call-back system in place?	91
		36) Is message authentication required in addition to user authentication?	91
		37) Is sensitive information prohibited from being transmitted over public lines unless the files are first encrypted?	91
		38) Is the organization aware of security features used by outside networks to which it connects? Are they acceptable?	92
		39) Are firewalls in use as needed?	92
		40) Are dial-in communication numbers protected from outsiders?	92

		41) Are modems disabled when not in use?	92
		42) Are modems always kept off automatic answer modes?	92
		43) Are modems only installed on computers in secure locations?	92
		44) Is Internet access granted to only those users who need it?	92
		45) Have all users been reminded that system use is only for approved activities?	92
		46) Are users required to sign Appropriate Use Agreements (see Chapter 3) before receiving access to the system?	92



CHAPTER 9

Protecting Your System: Network (Internet) Security

CHAPTER 9 IN A NUTSHELL:

Introduction to Network Security	pg 97
Commonly Asked Questions	pg 97
Policy Issues	pg 99
Network Security Countermeasures	pg 100
Closing Thoughts on Network Security	pg 102
Network Security Checklist	pg 103

Introduction to Network Security

Network security, especially as it relates to the biggest network of all, the Internet, has emerged as one of today's highest-profile **information** security issues. Many education organizations have already connected their computing **resources** into a single network; others are in the process of doing so. The next step for these organizations is to weigh the costs and benefits of opening a connection between their private networks (with their trusted **users**) and the unknown users and networks that compose the Internet.

Any connection of two or more computers constitutes a network. The Internet is simply a worldwide connection of computers and networks.

If, like many readers will, you have turned to this Network and Internet chapter first because it is your highest priority, be reminded that the information included in the other chapters of this document cannot be ignored. To reduce redundancy, security strategies from Chapters 1-8 and 10 that apply to Network and Internet security are not repeated in this chapter.

WARNING!

Discussions about Internet security can get technical. But while this issue is not for the faint of heart, it can and must be addressed before going on-line!

Commonly Asked Questions

Q. ***What is the Internet?***

A. The Internet is simply a worldwide connection of **computers** and networks. That is why this chapter is titled Network Security—because the Internet is, in its simplest terms, a very large network. If your

organization has its own network (which can be called an **Intranet**), you are basically working with a scale model of the Internet.

Q. ***Wouldn't an internal network be safer if it was never connected to an external network like the Internet in the first place?***

A. Yes, just as a person would be better protected from automobile accidents if he or she walked everywhere instead of driving. If walking (or avoiding external networks) meets your transportation (or computing and communication) needs, then it is a fine strategy. If, however, an organization wants to take full advantage of its equipment's powerful communication capabilities, then isolating itself from outside networks is a very poor plan. Instead, it would be better to connect with those networks that benefit the organization (including the Internet if that is the case), and then invest in, and implement, those protection strategies necessary to provide adequate security.

While employment sanctions and denial of access privileges are enforceable deterrents for internal users, they are not options for external Internet users.

Q. ***Why is there so much anxiety over connecting to the Internet?***

A. Internet **access** opens lines of communication with the world. But while this is potentially a powerful education tool, the admonition "beware of strangers" certainly applies. The major concern about being connected to the Internet is one of trust. Internet users and machines are not known to your network, don't fall within your policy and management jurisdiction, and may not share your opinions on appropriate use.

When you don't know who is accessing your network, you also don't know their intentions or level of technical expertise—thus, choosing to connect to the Internet has a significant impact on an organization's risk assessment (see Chapter 2).

It Really Happens!

Dan's files were losing data. There were no two questions about it—they had somehow been infected by a computer virus, and it deeply perplexed him. After all, hadn't he just downloaded a new virus scanner from the Internet precisely so this wouldn't happen. He was so baffled by the situation that he called Lisa, the office's computer guru to explain the mystery.

"I had been worried about my files accidentally getting infected by a virus for some time—you know, you read so much about it. So when I received this e-mail about getting a free virus scanner..."

Lisa interrupted, "What do you mean you received an e-mail? Who sent it?"

"That's the interesting part," Dan replied, "the guy who sent it said it was an electronic cold call. It seems that he was working for a software company and was trying to drum up business by offering a free virus scanner on a trial basis. I thought that it sounded weird, but when I visited the Web site, it all checked out."

Lisa also thought that it sounded odd and resolved to do some investigating. The first thing she did was run the software Dan had downloaded through her own virus scanner, one that had been verified for its authenticity. Sure enough, the scan revealed that Dan's download harbored a hidden virus—probably the one that was destroying his files. Now convinced that something very fishy was indeed going on, she decided to pay a visit to the Web site from which Dan had downloaded the software. When she got to it, the solution to the puzzle stared her in the face.

The Web site you have accessed belongs to Antivirus, Inc.

Antivirus, Inc. warns its customers that our sales staff is not, and never has been, responsible for sending random e-mail messages offering free trials of virus scanner software from this site. If you have received such an e-mail, you are the victim of a hacker who is masquerading as an agent of this company. This criminal has spoofed this Web site address and distributed a computer virus within software wrongly attributed to our product line. If you have downloaded this software, please e-mail Antivirus, Inc., and we will immediately furnish you an authentic version of our virus scanner for your temporary use while you disinfect your files. As co-victims of this crime, we understand your displeasure and apologize for any damage to your computing environment this incident has caused.

Be realistic! Recognize that as beneficial as the Internet can be for communicating and gathering resources, not everyone on it has your best interests in mind.

Policy Issues

Connecting to the Internet doesn't necessarily raise its own **security policy** issues as much as it focuses attention on the necessity of implementing security strategies properly. Internet security goals fall within two major domains. The first centers around protecting your networks, information, and other **assets** from outside users who enter your network from the Internet. The second deals with safeguarding information as it is being transmitted over the Internet.

Guidelines for security policy development can be found in Chapter 3.

Although it is not within the scope of this document to address in sufficient detail, policy-makers must consider what information can and cannot be posted to the Internet on, for example, a school's Web page.

Network Threats (Examples)

Examples of network **threats** include:

- Intentional acts of destruction (e.g., **address spoofing** and **masquerading**)
- Unintentionally destructive acts (e.g., accidental **downloading** of computer **viruses** and improper release of information)

As discussed more completely in Chapter 2, a threat is any action, actor, or event that contributes to risk.

If your brand-name operating systems, hardware, or software have any known security weakness built in, someone on the Internet will know about it. The Computer Emergency Response Team (CERT) Web site and comparable sites (see Appendix E) monitor weaknesses in computer software and post corrections. You should watch these sites—after all, hackers do.

A countermeasure is a step planned and taken in opposition to another act or potential act.

Select only those countermeasures that meet perceived needs as identified during risk assessment (Chapter 2) and that support security policy (Chapter 3).

Network Security Countermeasures

Because the Internet is relatively new, it isn't surprising that its standards are still being established and agreed upon. Consequently, it also shouldn't be surprising that its existing mechanisms for governing information exchanges are varied, not uniformly implemented, and, in many cases, not interoperable. Thus, it is only fair to admit that although the following **countermeasures** will greatly increase Internet security, more sophisticated and robust solutions remain on the horizon.

The following countermeasures address network security concerns that could affect your site(s) and equipment. These strategies are recommended when **risk assessment** identifies or confirms the need to counter breaches in the security of your network.

Countermeasures come in a variety of sizes, shapes, and levels of complexity. This document endeavors to describe a range of strategies that are potentially applicable to life in education organizations. In an effort to maintain this focus, those countermeasures that are *unlikely* to be applied in education organizations are *not* included here. If after your risk assessment, for example, your security team determines that your organization requires high-end countermeasures like retinal scanners or voice analyzers, you will need to refer to other security references and perhaps even hire a reliable technical consultant.

Many of these countermeasures get very technical very quickly. Non-experts need appreciate only the concepts, and then collaborate with technical staff to ensure that appropriate solutions are properly implemented.

- Protect Your Network from Outsiders:
  - *Implement applicable security recommendations as raised in previous chapters:* Solid defense against external Internet threats includes the proper implementation of relatively straightforward security measures like **encryption** software (Chapter 6), **virus scanners** (Chapter 7), **remote access** regulations (Chapter 8), and **passwords** (Chapter 8).
  - *Isolate your network through the use of a **firewall:*** Installing a firewall enables the organization to decide which types of messages should be allowed into the **system** from external sources (e.g., "nothing with identifiable virus coding" and "nothing with decryptor coding structures"). The actual installation and operation of the complex features requires expert technical assistance, but policy-makers can make informed decisions about product features all the same.
  - *Locate equipment and information that is intended for external users outside of the firewall:* If an organization's Web **server** is intended to provide information and services to the public, it should not be located on the private side of the firewall. Nor should it be able to access **confidential information** that resides inside the firewall. This way, if the public **Web** server should ever be compromised, confidential **information** is still protected.
- Protect Transmissions Sent over the Internet:
  - *Use Secure Sockets Layer (SSL) Servers to secure financial and information transactions made with a **Web browser:*** In a secure Web session, your Web browser generates a random encryption

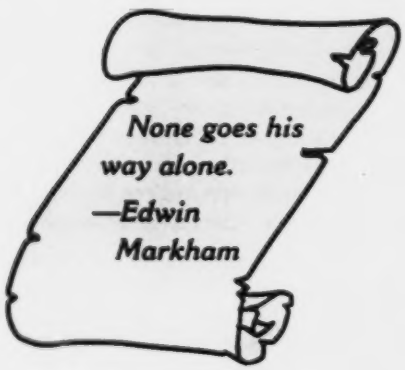
BEST COPY AVAILABLE

key and sends it to the Web site host to be matched with its public encryption key. Your browser and the Web site then encrypt and **decrypt** all transmissions.

- ***Authenticate** messages through the use of **digital signatures:** A digital signature amounts to a "fingerprint" of a message. It depicts the message such that if the message were to be altered in any way, the "fingerprint" would reflect it—thus making it possible to detect counterfeits. The converse, of course, is that if the "fingerprint" does not change during transmission, you can be confident that the message was not altered.
- *Authenticate messages through the use of **time stamps** or **sequence numbers:*** Another way to recognize when messages have been modified is to challenge the "freshness" of the message. This is done by embedding time stamps, sequence numbers, or random numbers in the message to indicate precisely when and in what order the message was sent. If a received message's time and sequence are not consistent, you will be alerted that someone may have tampered with the transmission.
- *Authenticate message "receivers" through the use of **digital certificates:*** By requiring an authentication agent or digital certificate, you force the person on the other end of the transmission to prove his or her identity. In the digital world, trusted third parties can serve as **certificate authorities**—entities that verify who a user is for you. In this way, digital certificates are analogous to a state-issued driver's license. If you trust the party that issues the certificate (e.g., the state or the certificate authority), then you don't need to try to verify who the user is yourself.
- *Encrypt all messages sent over the Internet (see Chapter 6):* As more and more messages are sent over larger and larger networks, information becomes increasingly vulnerable to assault. Encryption has become a leading tool to combat this **vulnerability.** Like other countermeasures, it can be very effective if used properly and regularly.

Digital signatures, time stamps, sequence numbers, and digital certificates are simply more examples of "authentication" procedures as discussed in Chapter 8.

Keep in mind that monitoring "authentication" procedures is accomplished by software. Once the systems are established, the user need only read the warning that the transmission did not maintain its integrity.



"Encryption" is a term used to describe when information is transformed into an unreadable format unless the reader possesses the appropriate key for decryption. The term "key" refers to a mathematical equation used to code (encrypt) information.

More Than You Need to Know about How Messages Are Encrypted

The process of encrypting and decrypting files depends on which encryption model your security solution employs. Encryption models vary in the number and size of the key(s) they use. As a general rule, the larger the key, the tougher it is to crack. There are two major types of encryption keys, systems currently in use:

- In a Single Key Encryption System, parties exchange a key known only to themselves, and use that key to encrypt and decrypt messages. The fundamental premise of this system is that parties must securely communicate the secret key to each other in order to encrypt and decrypt messages.
- The Public/Private Key Encryption System is based on a pair of mathematically related keys—a public key and a private key. Each key can decrypt information encrypted by the other. Your public key is used by anyone who wishes to send you an encrypted message or to verify your digital signature. Your private key is known only to you and is used to decrypt messages sent to you through the public key, or to digitally sign messages you are sending. This model allows for a much larger number of users than single key encryption because you need not have a separate key sent secretly to every trading partner.

Consensus appears to be moving the Internet toward a public/private key system in which third-party organizations that are entrusted as certificate authorities provide key management. Key management refers to the secure administration of encryption keys so that they become available to users only when and where they are required. This system is often referred to as the Public Key Infrastructure.

Policy-makers need not worry about the security of the entire Internet if they can be confident of the security of their connection to it.

Closing Thoughts on Network Security

The Internet simply is not secure unless you make it so. Luckily, basic Internet security is not beyond a non-technical person's ability to understand. By collaborating with **technical support staff** (or outside consultants if necessary), educational administrators can ensure that the near limitless amount of information and resources that exist on the Internet are available to system users without jeopardizing system integrity.

It should also be noted that network configurations are constantly changing. Many organizations are now relying upon Intranets for their internal communications. All security recommendations for the Internet can also be applied to Intranet applications.

Network Security Checklist

While it may be tempting to refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement security policy within and throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 9

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished? Yes	Accomplished? No	Check Points for Network (Internet) Security	Page
		Protect Your Network from Outsiders	100
		1) Have you fully implemented applicable security strategies as recommended in previous chapters?	100
		2) Has your network been isolated from the outside (e.g., the Internet) through the use of a firewall?	100
		3) Is equipment and information that is intended for "external" use logically located outside of your firewall?	100
		Protect Transmissions Sent over the Internet	100
		4) Is a Secure Sockets Layer (SSL) used to secure financial and information transactions made with a Web browser?	100
		5) Are messages authenticated via digital signatures?	101
		6) Are messages authenticated via time stamps or sequence numbers?	101
		7) Are message recipients authenticated by digital certificates?	101
		8) Are all messages sent over the Internet first encrypted?	101

CHAPTER 10

Training: A Necessary Investment in Staff

CHAPTER 10 IN A NUTSHELL:

Introduction to Training	pg 105
Commonly Asked Questions	pg 107
Targeting Training Efforts	pg 107
Training Goals	pg 109
A Sample Training Outline	pg 110
Training Frequency	pg 112
Closing Thoughts on Security Training	pg 113
Security Training Checklist	pg 113

Introduction to Training

Most staff in an education organization could probably offer a fairly accurate description of the term computer **virus** if asked. Viruses are big news. They are reported in the major media quite regularly, and, on occasion, are even headline stories. But ask those same staff members what **encryption software** is, or to suggest effective **disk backup** procedures, and they will most likely find themselves without much to say. While **threats** and catastrophes are newsworthy, day-to-day activities that protect **information** systems are often considered mundane.

When an organization allows television, magazines, and newspapers to be solely responsible for educating its staff, there is no logical reason for it to expect its employees to know how to implement even the most clearly stated of information technology security procedures. After all, while staff may have heard a thirty-second newsflash about the latest megavirus, they will not have been exposed to proper ways of using **computer** equipment and protecting information.

Organizations must reclaim the role of security educator from the mass media!

As mentioned throughout Chapters 5-9, all of the technological and procedural precautions in the world will be ineffective if they are not executed properly. But through well-conceived and committed security training programs, staff will be better prepared to avoid problems in the first place, minimize the damage of those problems that do arise, and maximize their contributions to **system** and information recovery when necessary. Without appropriate training (and associated reference tools), staff will instead be more likely to actually *contribute* to security **risk** through accidental but not necessarily malicious behavior. After all, most security problems are the result of unintentional human error. These mistakes will be less likely to occur when a well-intentioned employee has been properly trained.

It Really Happens!

The annual Management Information Systems (MIS) meeting was always a big deal. It was a great time for educators from across the state to meet and share fresh ideas and innovative projects. Dr. Lambeth spent the better part of the first day of the conference telling his fellow superintendents about the computerized student record system his staff had developed. He was very proud of the project and enthusiastically invited his counterparts to attend the presentation that his staff was giving later in the week.

When the day of the big presentation finally arrived, Dr. Lambeth was pleased to see several of his peers scattered throughout the large audience that had come to learn about the new system. His MIS Director, who was the lead speaker, began by offering a few introductory remarks before proceeding with a much-anticipated demonstration.

"Before we get started," he said into the microphone confidently, "we would like you to know that we've done everything we can to show you how this system really works. To this end, every step you see us take will be just as we do back in the office." He pushed a button on his computer and the overhead monitor displayed a student transcript. "For example, this transcript is exactly what we see when we access a student's record."

A hand was raised in the back of the room. The MIS Director acknowledged it. "Do you have a question?"

"Yes," a woman stood up and replied. "You accessed that sample student record very quickly. Are you running the software on a particularly powerful computer or have you just limited the number of records and files that you're using for the demonstration?"

Because system security demands information security and confidentiality, staff training must incorporate both topics. Refer to Appendix B for more information about FERPA.

The MIS Director smiled, pleased with the answer he was able to offer. "Neither. This equipment is no different than any other machines we run in our schools. And the records are 100% authentic school-level data. This demonstration re-creates our experiences in the real world accurately."

Another hand was raised. "You're not suggesting that the record we're looking at on the screen is that student's actual transcript. We can see her name, address, and grades."

The presenter interjected, "That's right, you're seeing the real thing, just like we do back in our district." Dr. Lambeth twisted in his seat uncomfortably. So did many other members of the audience, including several of the superintendents who had been encouraged to attend.

The next voice from the audience asked the MIS Director what everyone else was now wondering: "How can you interpret FERPA in a way that allows you to openly display that student's record?" Someone else added, "Especially considering that the presentation wouldn't be hindered if you just masked the parts of the transcript that identified that individual student. This is a public meeting. Anyone could walk in off the street and attend these sessions, including the parents of that young lady... who, we can all see, received a D in English last year."

The MIS Director was surprised by the criticism, "But I just wanted to make the demonstration realistic...." Dr. Lambeth interrupted the explanation. Despite his profound personal and professional embarrassment, the Superintendent stood up to apologize to the audience. "As you have duly noted, this demonstration of our student record system is flawed. It is apparent that we will need to share details about our project at another time when we are prepared to abide by laws such as FERPA and our own internal policies on protecting individual student record information. I am sorry, but this presentation is over."

BEST COPY AVAILABLE

Commonly Asked Questions

Q. ***If funds are scarce, isn't it better to implement security and postpone training rather than neglect security altogether?***

A. Neglecting security altogether is a terrible option. Unfortunately, attempting to implement security without appropriate training is not much better. A more effective approach is to rely upon the security priorities that are established in the organization's **risk assessment** (see Chapter 2) and then fund as many precautionary measures as can be implemented and trained for based on those priorities. While some **vulnerabilities** might be left unaddressed, the organization can have the peace of mind of knowing that at least those steps it has taken have a realistic chance of being properly implemented. It can then informally increase vigilance in areas of vulnerability it will not be able to address until additional funds become available.

Q. ***Can't training sometimes be overdone?***

A. Training can surely be overdone, although that is rarely the case in today's world of shrinking and non-existent training budgets. More often, training problems are a result of poor focus and poor timing. A training program should be focused on helping staff do their jobs better. It must be relevant to assigned duties and be presented in an understandable way that encourages employees to make security a part of their everyday routines. Similarly, training classes should be scheduled at convenient times for participants. If focus and timing are properly handled (i.e., sessions are helpful and convenient), it is much less likely that participants will complain about training being a burden.

Q. ***How does an organization know if its training program is effective?***

A. The most obvious way of measuring the effectiveness of security training is by monitoring the workplace for improved security performance. Scheduled and unscheduled testing of the security system is an excellent way of assessing its condition (see Chapter 4). Pre- and post-testing staff on training content is also an effective way of measuring improvements in security awareness, while yet another (and even more straightforward) way of evaluating training is to simply ask training participants what they thought of the experience. Since security depends heavily on the attitude and resulting commitment of staff, their opinion of the training, its relevance, and effectiveness is quite probably a good indicator of its success.

Training is a prerequisite for order, consistency, and realistic expectations of effective system defense.

Targeting Training Efforts

Who should receive security training? In a word, everybody! After all, a security breach affects each person in an organization. No matter the task a staff member is assigned, chances are that his or her role influences, and is influenced by, security policies and procedures. For example, people who clean offices need to know what can and can't be thrown away, and which rooms may or may not be off-limits. Teachers need to appreciate the necessity of protecting **passwords** and monitoring computer activity in their classrooms. Superintendents need to understand the importance of policy enforcement. And students need to be aware of proper floppy disk use and the viruses that can be spread if they fail to exercise due caution.

Staff technology training is also addressed in another National Center for Education Statistics publication, *Technology @ Your Fingertips* (see Appendix E).

How Does Security Affect the Workplace?

Security Area	Affected Activities
Physical strategies (Chapter 5)	Housekeeping/custodial, maintenance and operations, weekend/evening activities
Information/data protection (Chapter 6)	Public relations releases, research and evaluation reporting, interoffice mail delivery, disposal services
Software regulations (Chapter 7)	Administrative/clerical assistance, instructional delivery, library offerings
Access mechanisms (Chapter 8)	Access by Board members, substitute staff, students, and **telecommuters**
Network/Internet connections (Chapter 9)	**Internet** searches, site-to-site transmissions, public access (e.g., a school's **homepage**)

Every effort should be made to make security training as relevant as possible to day-to-day activities in the staff's work environment.

Exercises in the theoretical are not often well received by busy people. If staff members to whom training is directed don't think that it is practical, then the training will be seen as an additional burden. One way to make training sessions meaningful is to customize separate training programs to meet the needs of different types of staff and job groupings. For example, a training session designed to address security issues that affect clerical staff (e.g., software use and system **access**) has a good chance of being well-received by people who perform clerical duties because it is relevant to their jobs. Those same people might find a more general training session that includes significant periods of time discussing the management of students in computer labs less applicable to their duties and, consequently, less interesting.

It Really Happens!

Nancy had finally had enough of the training session. She raised her hand to ask the district's technology security manager a simple question: "Why am I here?"

Dan, the security manager, was taken by surprise. He thought through what he believed to be a straightforward answer to the question, and offered his reply. "Well, Nancy, protecting the district's information and equipment is important to us as an organization, and we must all do our part."

"I understand that," Nancy interrupted him, "and I agree with it. But I've been here for over an hour listening about how to transmit transcripts to colleges, how to mask individual identifiers in press releases, and how to develop documentation when programming new software. In twelve years as a classroom teacher, I've not done one of those things, and I seriously doubt that I will in the next twelve years either. What I do need to do as a teacher is submit end-of-the quarter grades... by Thursday. Going to the teachers' lounge and doing so would be a much better use of my time than this training class."

Dan hadn't expected such an attack on his training session, and explained that the time would prove worthwhile for everyone if, as a group, the audience could be patient. "Nancy, I pride myself on being thorough.

I plan to address electronic grade book issues in the next fifteen minutes or so. Will that satisfy you?"

Nancy sensed that Dan was put off by her comments. She didn't want to be unfriendly but felt strongly about her point. "I'm glad that you're planning to talk about the security of our electronic grade books. It is an important issue to many of us, especially the teaching staff. But it would have been better for each of the twenty or thirty teachers here if you would have just told us that you wouldn't be getting to the part that matters to us until the end of the session. We could have then shown up at that point and wouldn't have felt like the rest of this had been a waste our time. I'm sorry to be so blunt about it, Dan, but you need to hear this so that you can plan the next training a little more efficiently. Please accept this as constructive criticism, because you do a great job with the training material when it is relevant—but, like teaching, it doesn't matter how well you present the material if the students don't see any point to it."

Each organization will be different in terms of the types of job-alike training sessions that it might want to offer, but the following groups are common to many organizations and are logical target audiences for security training.

Typical Job-Alike Training Groups

- High-Level Administrators
- Middle Managers
- Teachers
- Students
- Data Processing/MIS Professionals
- Clerical Staff
- Custodial Staff
- Paraprofessionals
- Volunteers
- Other Support Staff

"Job-alike" training is used to describe a training program in which sessions are designed for specific user groups based on the similarities of their job duties.

Training Goals

Even when information security training is customized to meet the needs of specific **user** groups through a job-alike approach, every session, no matter the target audience, should have the following goals:

Goal 1: Raise staff awareness of information technology security issues in general.

Goal 2: Ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security.

Goal 3: Explain organizational security policies and procedures.

Goal 4: Ensure that staff understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.

Goal 5: Train staff to meet the specific security responsibilities of their positions.

Goal 6: Inform staff that security activities will be monitored.

Goal 7: Remind staff that breaches in security carry consequences.

Goal 8: Assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making).

Goal 9: Communicate to staff that the goal of creating a **"trusted system"** is achievable.

Goal 5 stands out as key when customizing for job-alike training.

Each of the above goals should provide the same types of information to all employees without regard to their job-alike grouping—the significant exception to this point is Goal 5, in which security responsibilities are explained as they specifically relate to participant duties.

What a Wonderful World It Would Be...

In the broader sense of computer use, staff should learn to:

1. Never use a computer as a tool to harm other people.
2. Never interfere with other people's computer work.
3. Never snoop around in other people's computer files.
4. Never use a computer to steal.
5. Never use a computer as a tool for misrepresenting information.
6. Never use other people's computer resources without their permission.
7. Never lose sight of the social consequences of the work being done with the computer.

This list is adapted from the *Code of Conduct for Computer Users* as developed by The Computer Ethics Institute (see Appendix E).

While security training focuses on improving the implementation of security procedures, training staff on basic computer use also contributes to system security, and is vital.

Train staff to control the system responsibly so that the system doesn't control them.

A Sample Training Outline

Allowing for customizing to meet the requirements of job-alike training, the following outline provides an overview of how a typical security training session could be effectively structured:

I. Security overview
   - A. What is information security?
   - B. Why does it matter?

II. Federal laws
   - A. FERPA overview
   - B. FERPA relevance and application (include specific examples that relate to audience duties)

See Chapters 1-3 for information about FERPA and other policy concerns.

III. State and local laws, regulations, and standards

A. Statute, regulation, and standard overview

B. Statute, regulation, and standard relevance and application (include specific examples that relate to audience duties)

IV. The organization's security plan

A. Risk assessment findings

1. **Assets**
2. Threats
3. **Vulnerabilities**

B. Organizational security policies, procedures, and regulations (focus on those related to audience duties)

1. Physical security regulations
2. Information security regulations
3. Software security regulations
4. User access security regulations
5. **Network security regulations**

C. Security administration

1. Expectations
2. Monitoring activities
3. Authorities
4. Enforcement and consequences
5. Avenues of communication

V. On-the-job training (i.e., "Here's what you really need to do...")

A. Explanations

1. Turning the computer on and off
2. **Logging in** and out
3. Changing passwords
4. And so on

B. Demonstrations

1. Turning the computer on and off
2. Logging in and out
3. Changing passwords
4. And so on

C. Testing

1. Turning the computer on and off
2. Logging in and out
3. Changing passwords
4. And so on

D. Monitoring

1. Turning the computer on and off
2. Logging in and out
3. Changing passwords
4. And so on

Ongoing training is essential for keeping staff focused. Distributing handouts, "cheat" sheets, and other reference materials is an effective way of supporting staff long after a training session is over and everyone is back on the job.

One way of illustrating the rationale for security regulations is to have staff look at the vulnerabilities of an *un*secured system from the perspective of a potential intruder, and then consider how much more difficult it would be to attack a secured system.

True training entails more than telling employees what they can and cannot do. Simply saying "back up your work because it is a rule" does not educate staff. Instead, rationale for policies and regulations should be explained to employees. This does not require every step of the organization's risk assessment to be rehashed, as much as it means that procedures should be justified and made relevant to the audience's work. For example, instead of telling staff that they must protect their passwords, an explanation of what a malicious user could do while posing as an innocent staff person (through the use of their password) might be more effective—after all, very few people are willing to allow themselves to be made someone else's scapegoat! By describing how security protects users as well as the system and organization, security training can become an effective way of garnering staff support and ensuring that policies and regulations are implemented.

Users must be reminded what is at risk if the system is not effectively secured, including:

1. **Organizational** resources and reputation
2. **Confidential information** that students trust school **employees** to protect
3. Personal work files that would need to be re-created at considerable staff effort

Training Frequency

How often staff should be trained (and when) is an issue that requires significant consideration. A good rule of thumb is that all newly hired employees should undergo general organizational security training as a part of their orientation before they actually assume their duties. Similarly, job-alike or comparable training should be required of all staff (new or old) at the onset of initiating a security program.

An overwhelming three-hour session in which staff learn little is a poor use of time compared to three more manageable *forty-five minute* sessions in which they retain a lot.

After initial training sessions have been offered, it is important to continue to educate staff regularly. Ongoing efforts allow for major points to be reemphasized, while also providing trainers with opportunities to break complex issues into manageable pieces of information that staff can more easily comprehend. For example, the concept of user **authentication** may be more readily understood by staff if it is broken into separate sessions on in-house log-in procedures (session one) and **remote access** (session two).

Training surely demands the dedication of time and resources, but the alternative usually exacts a far higher toll!

The secret of education lies in respecting the pupil. —*Emerson*

Closing Thoughts on Security Training

Security policies and regulations are "living" concepts. That is, they can change depending on circumstances. If, for example, an improved type of encryption software is released, an organization and its employees might need to learn how to use it. Similarly, if a new **data** collection is initiated, policy-makers will need to evaluate the confidentiality of the information it generates. In both cases (and countless other examples), having a training mechanism in place to inform and educate staff is not only very valuable, but a real necessity—because a staff that is not properly trained limits, and perhaps even negates, the potential effectiveness of even the best devised security strategies.

Shortchanging security training is the equivalent of short-changing security itself. Don't undermine an investment in equipment, software, and policy development by failing to also invest in your people.

Security Training Checklist

While it may be tempting to simply refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement **security policy** throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs—a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 10

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Accomplished?		Check Points for Security Training	Page
Yes	No		
		1) Have decision-makers committed to comprehensive training as a necessary part of implementing any information technology security program?	105
		2) Is training targeted at everyone in the organization to the degree their activities warrant?	107
		3) Are training sessions customized to meet the needs of specific user groups, a concept referred to here as "job-alike" training (see Point 8 below)?	109
		4) Is training designed to raise staff awareness of information technology security issues in general?	109

		5) Is training designed to make staff aware of local, state, and federal laws and regulations governing information confidentiality and security?	109
		6) Is training designed to explain organizational security policies, procedures, and regulations?	109
		7) Is training designed to ensure that staff understand that security is a team effort and that each person has an important role to play?	109
		8) Is training designed to help staff meet the specific security responsibilities of their positions?	109
		9) Is training designed to inform staff that security activities must and will be monitored?	109
		10) Is training designed to remind staff that breaches in security carry consequences for the individual and the organization?	109
		11) Is training designed to encourage staff to report potential and actual security breakdowns and vulnerabilities?	109
		12) Is training designed to communicate to staff that the goal of creating a "trusted" system is achievable?	109
		13) Has the sample training outline been reviewed as an aid in helping the organization's training planners develop their own program?	110
		14) Is the rationale for security policies and regulations explained as a part of training?	112
		15) Are all new staff trained before they assume their duties?	112
		16) Will staff training be initiated at the onset of implementing any security program?	112
		17) Is staff training and related support information provided on an ongoing basis?	112
		18) Have decision-makers recognized that a security policy is a "living"concept and, therefore, requires frequent reevaluation?	113

BEST COPY AVAILABLE

Appendix A

Additional Resources about Computing

This document endeavors to maintain its focus on information and technology *security*, and is not intended to explain the technical operations of computers, systems, or networks. For those readers who are interested in how computers operate, are configured, and are networked, the following is a list of on-line and print resources that address those and other technical issues.

On-line Resources

A Search Engine - http://www.yahoo.com/computers
This site provides a directory of computer-related on-line resources.

A Dictionary - http://whatis.com
Whatis.com offers an on-line dictionary of computer terms.

A Self-Study Course - http://www.mkdata.dk/english
This site, titled *Click & Learn*, offers a self-study course about PCs, their hardware, and internal architecture. It is an excellent technical resource.

Frequently Asked Questions - http://kbl.ucs.indiana.edu
This Indiana University site, titled *Knowledge Base*, is a database of common technology questions that arise at the University, but is applicable to outsiders as well. It, too, is an excellent resource.

Print Resources

Freedman, A. (1996). *The Computer Desktop Encyclopedia*. New York, NY: Amacom, Inc. (ISBN: 0-8144-0012-4)

Maran, R. (1996). *Teach Yourself Computers & the Internet Visually*. Foster City, CA: IDG Books Worldwide, Inc. (ISBN: 0-7645-6002-6)

Rosch, W.L. (1997). *Hardware Bible: Your Complete Guide to All Types of PC Hardware*. Indianapolis, IN: Sams Publishing. (ISBN: 0-672-30954-8)

White, R. (1997). *How Computers Work*. Emeryville, CA: Ziff-Davis Press. (ISBN: 1-56276-546-9)

Appendix B

FERPA FACT SHEET

Family Educational Rights and Privacy Act of 1974 (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a Federal law designed to protect the privacy of a student's education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student, or former student, who has reached the age of eighteen or is attending any school beyond the high school level. Students and former students to whom the rights have transferred are called eligible students.

- Parents or eligible students have the right to inspect and review all of the student's education records maintained by the school. Schools are not required to provide copies of materials in education records unless, for reasons such as great distance, it is impossible for parents and eligible students to inspect the records. Schools may charge a fee for copies.
- Parents and eligible students have the right to request that a school correct records believed to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record commenting on the contested information in the record.
- Generally, the school must have written permission from the parent or eligible student before releasing any information from a student's record. However, the law allows schools to disclose records, without consent, to the following parties:
  - School employees who have a need-to-know
  - Other schools to which a student is transferring
  - Certain government officials in order to carry out lawful functions
  - Appropriate parties in connection with financial aid to a student
  - Organizations doing certain studies for the school
  - Accrediting organizations
  - Individuals who have obtained court orders or subpoenas
  - Persons who need to know in cases of health and safety emergencies
  - State and local authorities, within a juvenile justice system, pursuant to specific state laws

Schools may also disclose, without consent, "directory" type information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendances. However, schools must tell parents and eligible students about directory information and allow parents or eligible students a reasonable amount of time to request that the school not disclose directory information about them.

Schools must notify parents and eligible students of their rights under this law. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information or technical assistance, call (202) 260-3887 or TDD (202) 260-8956, or contact:

Family Policy Compliance Office
U.S. Department of Education
600 Independence Avenue, S.W.
Washington, D.C. 20202-4605

Appendix C

Related NCES Publications

(These publications are available through the U.S. Government Printing Office, Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328. More information can also be found through the NCES World Wide Web Home Page at http://nces.ed.gov.)

Technology @ Your Fingertips

A Guide to Implementing Technology Solutions for Education Agencies and Institutions (available on-line at http://nces.ed.gov/pubs98/98293.pdf)

Technology @ Your Fingertips describes a process for getting the best possible technology solution for an education organization. It presents a step-by-step approach to identifying an organization's technology needs, evaluating its options, and acquiring and implementing its solution. The document does not dictate specific equipment and software that must be purchased. Rather, it arms its readers with a process they can use to customize technology solutions to their organization's specific needs.

The book is not aimed at "technical" staff who may already be familiar with many of the concepts and much of the information it contains. The guidelines are, instead, intended for those who have been given the responsibility of purchasing and installing computers and networking technology for an education organization (or the responsibility of supervising computers and network technology once they have already been established). The guidelines are expected to be of most use to persons in schools or districts. However, they are also applicable to other types of education settings, including colleges, universities, libraries, and state education agencies.

Because the world of technology is very broad, the document focuses on computer and networking technology—primarily software used to meet administrative and instructional needs, and the hardware, networking, and support to allow it to function properly. It also addresses budgetary and human resources concerns. It is written in non-technical language and includes references to numerous other resources.

Protecting the Privacy of Student Records

Guidelines for Education Agencies (available on-line at http://nces.ed.gov/pubs97/97527.pdf)

School districts maintain and use personal information for a variety of educational purposes. Students and their parents entrust schools with their personal information with the expectation it will be used to serve the students effectively and efficiently. To protect the privacy of families whose children are in school, states and the federal government have established strong legal statutes to secure information that schools maintain in student education records. Thus, agency and school staff are not only ethically, but also legally, responsible for safeguarding student information in order to protect the privacy of students and their families.

Protecting the Privacy of Student Records was written to help state and local education agencies and schools develop adequate policies and procedures to protect information about students and their families from improper release, while still satisfying the need for school officials to make sound management, instructional, and service decisions. Suggested audiences include state education agency staff, state and local policy-makers, school district staff, school administrators and staff, program and support services staff, technical staff, and teachers and other school-based support professionals.

Appendix D

Sample Acceptable Use Agreements

The following are *samples* of agreements that organizations can refer to as they develop Information and Technology Security Agreements and Internet Acceptable Use Agreements for students, staff, contractors, and other individuals who are to be given access to equipment, information, or networks. These samples have been compiled from existing agreements that are currently in use in schools and local education agencies. The conditions they specify may or may not be applicable to all potential readers, and are, therefore, presented only as a resource. They do not in any way represent a standard or an agreed-upon convention.

Information and Technology Security Agreements

These *sample* Information and Technology Security Agreements do not take the place of security policies, guidelines, and procedures that are customized to meet the specific needs of the organization (the development of which is detailed throughout the body of the document). In fact, precisely the opposite is true. The following agreements are designed to certify that the signer acknowledges that relevant security policies, guidelines, and procedures have been developed by the organization and subsequently presented to the signer in a clear and meaningful way that outlines what their security responsibilities will be. These agreements are, therefore, simply the formal mechanisms by which the signer acknowledges that he or she is aware of the information and technology security policies, guidelines, and procedures, and agrees to abide by them.

Employee Information and Technology Security Agreement

I acknowledge that [name of organization]'s information and technology security policies, guidelines, and procedures have been made available to me for adequate review and consideration. I also certify that I have been given ample opportunity to have any and all questions about my responsibilities addressed. I am, therefore, aware that I am accountable for information and technology security procedures as they govern the acceptable performance of my job. I understand that failure to abide by any and all policies, guidelines, and procedures can result in organizational, civil, or criminal action and/or the termination of my employment.

Signature: _____ Printed Name: _____

Job Title: _____ Date: _____/_____/_____

Contractor/Consultant/Outsider Information and Technology Security Agreement

I acknowledge that [name of organization] has provided me with adequate time to review and consider the information and technology security policies, guidelines, and procedures it deems applicable to responsibilities I am undertaking on behalf of [name of organization], regardless of my employment status. I also certify that I have been given ample opportunity to have any and all questions about my responsibilities addressed. I am, therefore, aware that I am accountable for those information and technology security procedures as they relate to my work for, or on the behalf of, [name of organization]. I understand that failure to abide by any and all policies, guidelines, and procedures can result in organizational, civil, or criminal action and/or the termination of my relationship with [name of organization].

Signature: _____ Printed Name: _____

Affiliation: _____ Date: _____/_____/_____

Internet Acceptable Use Agreements

The following *sample* Internet Acceptable Use Agreements specify common requirements and prohibitions for Internet use by (1) organization staff, (2) high school students, and (3) elementary, middle, or junior high students. A sample Parent/Guardian Internet Permission Letter is also included and should accompany any Acceptable Use Agreements given to minors (i.e., most students).

Staff Guidelines for Acceptable Internet Use

The following statements guide acceptable staff use of Internet resources:

1. Staff must sign a valid Employee Information and Technology Security Agreement that affirms that they acknowledge and agree to abide by all organizational policies, guidelines, and procedures that govern computer, network, Internet, and information use.
2. Staff may not damage or mistreat equipment or facilities under any circumstances.
3. Staff may not intentionally waste computer resources.
4. Staff may not employ the network for personal financial gain or commercial purposes.
5. Staff may not violate regulations prescribed by the network provider.
6. Staff may not engage in practices that threaten the integrity of the network (e.g., knowingly download files that contain a virus).
7. Staff may not engage in personal business that is unrelated to the mission of the organization or the performance of their job.
8. Staff may not write, use, send, download, or display obscene, threatening, harassing, or otherwise offensive messages or pictures, including pornography.
9. Staff may not use the equipment or network for any illegal activities, including the violation of copyright laws and software piracy.
10. Staff may not load or copy any software or other programs to or from organizational equipment unless permission is explicitly granted by an authorized party (e.g., the network administrator or technology committee).
11. Staff may not use anyone else's password, nor may they share their password with others.
12. Staff may not trespass into anyone else's folders, documents, or files.
13. Staff may not disclose anyone else's personal information (e.g., address, phone number, or confidential information), including and especially that belonging to students, community members and families, or fellow employees.

Staff should also be aware that communication over a network is frequently recognized as public by its very nature. Therefore, general rules and standards for professional behavior and communications will apply at all times. In an effort to maintain system integrity and to ensure responsible use, files and communications can and will be monitored. *Staff should not under any circumstances expect that messages or files that are created, modified, transmitted, received, or stored on organizational equipment are private.*

Staff Member: "I have read these Staff Guidelines for Acceptable Internet Use and agree to use the Internet and all associated equipment and information in a way that is consistent with these guidelines. I understand that failure to do so will result in the loss of my Internet privileges and other disciplinary action as deemed appropriate by organizational officials."

Signature: _____

Printed Name: _____

Date: _____/_____/_____

High School Student Guidelines for Acceptable Internet Use*

Access to computer, network, and Internet equipment and software at [name of organization] offers students an almost unlimited source of resources and information to support their educational development. Under staff supervision, students will have the privilege of searching the Internet for expert resources, communicating with other students from around the world, and participating in various distance-learning activities. But with the use of these powerful tools comes great responsibility. Access to these resources is a privilege, not a right. Students are advised that some Internet sites may contain offensive or inappropriate information, messages, and pictures for an educational setting. [Name of organization] does not condone or permit the use of such material. Therefore, access to the Internet is granted only on the condition that a student agrees to be accountable for appropriate use of these resources. In addition to all information and technology security policies, guidelines, and procedures that govern computer and network use at [name of organization], the following statements guide acceptable use of Internet resources by all high school students:

1. Students may not use equipment or facilities in a way that is inconsistent with the general rules of conduct that govern student behavior at [name of organization].
2. Students may not damage or mistreat equipment or facilities under any circumstances.
3. Students may not intentionally waste computer resources.
4. Students may not employ the network for personal financial gain or commercial purposes.
5. Students may not violate regulations prescribed by the network provider.
6. Students may not engage in practices that threaten the integrity of the network (e.g., knowingly download files that contain a virus).
7. Students may not write, use, send, download, or display obscene, threatening, harassing, or otherwise offensive messages or pictures, including pornography.
8. Students may not use the equipment or network for any illegal activities, including the violation of copyright laws and/or software piracy.
9. Students may not load or copy any software or other programs to or from organizational equipment.
10. Students may not use anyone else's password, nor may they share their password with others.
11. Students may not trespass into or in any way alter anyone else's folders, documents, or files.
12. Students may not disclose anyone's personal information (e.g., address, phone number, or confidential information), including their own or that belonging to a fellow student, community members and families, or staff member.

Students should be advised that in an effort to maintain system integrity and to ensure responsible use, files and communications can and will be monitored. *Students should not under any circumstances expect that messages or files that are created, modified, transmitted, received, or stored on organizational equipment are private.* Students who violate any of the above conditions will be subject to the suspension or termination of their Internet and computing privileges, as well as other disciplinary action as determined appropriate by school officials.

Student: "I have read these Student Guidelines for Acceptable Internet Use and agree to use the Internet and all associated equipment and information in a way that is consistent with these policies. I understand that failure to do so will result in the loss of my Internet privileges and/or other disciplinary action as deemed appropriate by school officials."

Signature: _____

Printed Name: _____

Date: _____/_____/_____

*This agreement should be accompanied by a signed and dated ***Parent/Guardian Internet Permission Letter.***

Elementary, Middle, and Junior High School Student* Guidelines for Acceptable Internet Use

Access to the Internet is offered to help students learn. With the help of teachers, the Internet can be used for researching, studying, and communicating. But the Internet also includes some information that is not appropriate for students and the school environment. Therefore, students must agree to behave properly when using this powerful learning tool. The following rules should help a student understand what type of behavior is expected of Internet users.

1. Students must be kind and polite when using the Internet.
2. Students must use Internet equipment only for school-related activities.
3. Students may use the Internet only when they have permission from a teacher.
4. Students should not damage or mistreat computer equipment under any circumstances. This includes trying to "fix" plugs, cables, or other parts of the equipment. Leave that to your teacher.
5. Students should not access files that do not belong to them.
6. Students should not copy, download, or install any software or programs to or from school computers.
7. Students must not write, send, download, or display obscene, threatening, harassing, or otherwise harmful messages or pictures.
8. Students must not share their personal address, phone number, or any other contact information over the Internet. They must not share information about other people either, including friends, fellow students, or teachers.
9. Students should be aware that e-mail and Internet use can and will be monitored and therefore is not private.
10. Students must obey all rules that normally govern their behavior at school when using the Internet.

Student: "I have read or been read these Student Guidelines for Acceptable Internet Use and agree to use the Internet in a way that is consistent with these policies. I understand that failure to do so will result in the loss of my Internet privileges and/or other disciplinary action as deemed appropriate by school officials."

Student Signature: _____

Printed Name: _____

Date: _____/_____/_____

*This agreement should be accompanied by a signed and dated ***Parent/Guardian* Internet Permission Letter**

Parent/Guardian Internet Permission Letter*

Dear Parent/Guardian,

We are pleased to offer students at [insert name of organization] access to the Internet. The Internet is a global computer network that is used by educators, students, government, business, and a host of other organizations and individuals to communicate electronically. As a learning resource, the Internet is similar to books, magazines, video, CD-ROM, and other information sources, except that it quite literally enables students to explore countless numbers of computers, networks, libraries, and databases from throughout the world. Use of the Internet for educational purposes will assist students in identifying resources, gathering information, and developing the technical skills they will need for life and work in the twenty first century.

It must be made clear, however, that although your child's use of the Internet will be supervised, we cannot guarantee that a student will not be able to access information that you might consider to be objectionable. Therefore, it is imperative that both students and their parents be aware of each individual student's responsibility for ethical and appropriate Internet use. Just as students are expected to behave properly in the classroom and school hallways, they will also be required to behave responsibly while using school computers and networks. Technical resources are provided to help students meet their information needs within the context of teacher-planned assignments and school-sponsored activities. Access to these resources, however, is a privilege, not a right. It is permitted only on the condition that a student agrees to act in a responsible manner. School staff reserve the right to suspend or terminate the use of the Internet by any student who violates these policies. Similarly, Internet use is subject to all policies and regulations that govern student behavior in other school activities.

Please review the attached Student Guidelines for Acceptable Internet Use agreement that your child will be required to read and sign before being granted Internet access. We encourage you to take advantage of this opportunity to discuss your family's values with your child and how they, too, should affect Internet use. Please feel free to contact [name and title of organizational contact person] at [contact information] if you have any questions about Internet use or Internet policies at [name of organization]. You are not required to grant permission for your child to access the Internet, but we firmly believe that Internet use in an approved educational setting, with specific educational objectives, and under appropriate supervision will prove to be a positive learning experience for your child.

Parent/Guardian: "I have read this letter and the Student Guidelines for Acceptable Internet Use, and give permission for my son/daughter to use the Internet at [name of organization]."

Parent/Guardian Signature: _____

Printed Name: _____

Date: ___/___/___

Student: "I have read or been read the Student Guidelines for Acceptable Internet Use as attached and agree to use the Internet in a way that is consistent with these policies. I understand that failure to abide by these policies will result in the loss of my Internet privileges and/or other disciplinary action as deemed appropriate by school officials."

Student Signature: _____

Printed Name: _____

Date: ___/___/___

*Any *minor* should present written permission from a parent/guardian before receiving access the Internet.

Appendix E

Bibliography and Selected Reference Materials

Print Documents

Alexander, M. (1996). *The Underground Guide to Computer Security*. Reading, MA: Addison-Wesley Publishing Company.

California Department of Education. (1994). *K-12 Network Technology Planning Guide: Building the Future (Draft)*. Sacramento, CA: California Department of Education.

CAUSE. (1997). *Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities*. Boulder, CO: CAUSE.

Cobb, S. (1996). *The NCSA Guide to PC and LAN Security*. New York, NY: McGraw-Hill, Inc.

Crowe, Elizabeth P. (1994). *The Electronic Traveller: Exploring Alternative Online Systems*. Tab Books. (ISBN: 0830644989).

Dern, D.P. (1994). *The Internet Guide for New Users*. New York, NY: McGraw-Hill, Inc.

Idaho State University, Department of Computer Information Systems. (1988). *Information Security Modules*. Unpublished presentations from a U.S. Department of Defense-sponsored workshop.

Levine, J.R., Baroudi, C. and Levine-Young, M. (1995). *The Internet for Dummies (3rd Edition)*. Foster City, CA: IDG Books Worldwide, Inc.

National Security Agency, Information Systems Security Organization. *Computer Security in a Networked Society (Training Brief)*. Presented at the National Center for Education Statistics' Summer Data Conference, July 1996.

Russel, D. and Gangemi, G.T. (1991). *Computer Security Basics*. Sebastopol, CA: O'Reilly & Associates.

Strang, D. and Moon, S. (1993). *Network Security Secrets*. San Mateo, CA: IDG Books Worldwide, Inc.

Time-Life Books (Eds). (1986). *Computer Security*. Alexandria, VA: Time-Life Books.

U.S. Bureau of the Census. (1996). *Handbook for Information Technology Security*. Unpublished internal use document.

U.S. Department of Commerce. (1975). *Computer Security Guidelines for Implementing the Privacy Act of 1974*. Washington, DC: Government Printing Office.

U.S. Department of Education, National Center for Education Statistics. (1997). *Protecting the Privacy of Student Records: Guidelines for Education Agencies*, NCES 97-527. Washington, DC: Government Printing Office.

U.S. Department of Education, National Center for Education Statistics. (1997). *Technology @ Your Fingertips*, NCES 98-293. Washington, DC: Government Printing Office.

Available On-Line Resources

American Association of School Administrators (http://www.aasa.org). This site includes appropriate use policies as well as technology plans and other planning resources.

Computer Crime Research Resources (http://mailer.fsu.edu/~btf1553/ccrr/states.htm). This site provides lists of, and links to, state statutes (by state) pertaining to crimes involving computers and information.

Computer Ethics Institute (CEI) (www.brook.edu/its/cei/cei%5Fhp.htm). CEI offers an advanced forum and resource for identifying, assessing, and responding to ethical issues associated with the advancement of information technologies in society.

Computer Emergency Response Team (CERT) Coordination Center (http://www.cert.org). CERT studies Internet security vulnerabilities, provides incident response services to sites that have been victims of attack, publishes a variety of security alerts, researches security and survivability in wide-area-networked computing, and develops information to help you provide security at your site.

National/International Computer Security Association (NCSA/ICSA) (http://www.ncsa.com). The NCSA/ICSA is an organization dedicated to improving security and confidence in global computing through awareness and the continuous certification of products, systems, and people. It offers a wide range of security publications for sale included under topics such as Communications and Security, Computer Privacy and Ethics, Computer Viruses, Cryptography, Disaster Recovery, Firewalls and Internet Security, General Security, and Network Security.

National Institute of Standards and Technology (NIST) Computer Security Resource Clearinghouse (http://csrc.nist.gov). The NIST Computer Security Division offers guidance and technical assistance to government and industry in the protection of unclassified automated information systems. The Computer Security Resource Clearinghouse provides an online archive of useful information available via the World Wide Web.

National Security Institute (http://nsi.org/compsec.html). This site offers a wide range of security-related information under the headings Alerts and Warnings, Threats, Manager's Guides, Communication and Encryption, Papers and Programs (and FAQs), Government Standards, Internet, Mailing Lists and News Groups, and Links.

Network/Computer Security Technology (http://huitzilo.tezcat.com/web/security). This site is intended to provide an access point to security-related resources across the Internet.

U.S. Department of Education, Office of Educational Technology (http://www.ed.gov/Technology). This site offers access to information on a range of U.S. Department of Education initiatives that promote the use of technology in schools, libraries, and communities to achieve its mission of ensuring equal access to education and promoting educational excellence throughout the nation.

World Wide Web Security FAQ (Frequently Asked Questions) (http://www.w3.org/Security/Faq). This FAQ list attempts to answer some of the most frequently asked questions relating to the security implications of running a Web server and using Web browsers.

Appendix F

Citations

NOTE: Appendix E contains bibliographical information for each document listed in these citations.

No.	Reference
1.	Text adapted from *Computer Security Basics*, p. 20
2.	Bullets adapted from *Network Security Secrets*, p. 908
3.	*Computer Security in a Networked Society* (NSA Training Brief), p. 31
4.	Bullets adapted from *Computer Security Guidelines*, p. 9
5.	Bullets adapted from *Information Security Modules*, p. 32
6.	Text adapted from *Computer Security Basics*, p. 105
7.	Bullets adapted from *Computer Security Guidelines*, p. 9
8.	Box adapted from *Information Security Modules*, p. 73
9.	Bullets adapted from *Network Security Secrets*, p. 890
10.	Bullets adapted from *Network Security Secrets*, p. 890
11.	Bullets adapted from *The Underground Guide to Computer Security*, p. 199
12.	Bullets adapted from *Network Security Secrets*, p. 830
13.	Bullets from Census *Handbook for Information Technology Security*, p. 36
14.	Bullets adapted from *Network Security Secrets*, p. 833 AND *The Underground Guide to Computer Security*, p. 155
15.	Bullets from *Network Security Secrets*, p. 828
16.	Bullets adapted from *NCSA Guide to PC and LAN Security*, p. 323
17.	Bullets adapted from *Information Security Modules*, p. 22
18.	Some bullets adapted from *The Network Security Secrets*, p. 274
19.	Some bullets adapted from *Network Security Secrets*, p. 162
20.	Box definitions from *Information Security Modules*, p. 31
21.	Sidebar from *Information Security Modules*, p. 77
22.	Some bullets adapted from Census *Handbook for Information Technology Security*, p. 20
23.	Adapted from *Computer Security Basics*, p. 61

Glossary

(Note: All terms are defined based on their use *in this document.)*

Acceptable use policy- A policy designed to limit the ways in which a computer or network can be used. Acceptable Use Policies (AUPs) usually include explicit statements about the required procedures, rights, and responsibilities of a technology user. Users are expected to acknowledge and agree to all AUP stipulations as a condition of system use, as should be certified on the AUP by the user's signature.

Access- To make use of a technology resource (e.g., a computer or network). Also, to make use of the information or data that reside on a computer or network. See also **Remote access**.

Address spoofing- See **Spoofing**.

Administrative software- Computer programs that are used to expedite the storage and use of data and information. Examples of administrative software include student records systems, personnel records systems, and transportation mapping packages. See also **Computer program, Software**, **Instructional software**, and **Application software**.

Antivirus software- Computer programs designed to detect the presence or occurrence of a computer virus. The software subsequently signals an alert of such a detection via any of a variety of mechanisms and, in many commercial products, can then be used to delete the virus. See also **Computer program**, **Software**, **Virus**, and **Virus scanner**.

Application software- Computer programs that are used to accomplish specific tasks not related to the functioning of the computer itself. In broad categories, both administrative software and instructional software are types of application software. More specific examples include word processing, spreadsheet, and database software. See also **Computer program**, **Software**, **Administrative software**, **Instructional software**, and **Operating system software**.

Appropriate use policy- See **Acceptable use policy**.

Asset- Real property, including information, software, and hardware (i.e., those things an organization needs to protect). Information and technology security requires that all assets be identified through the process of risk assessment in order to appropriately design security strategies. See also **Information, Software, Hardware,** and **Risk assessment**.

Attack- An attempt to violate information and technology security. See also **Asset, Countermeasure, Risk, Threat, Vulnerability,** and **Risk Assessment**.

Audit- See **Security audit**.

Audit trail- A detailed record of user transactions that chronicles all system activity (from each user's log-on to log-off and everything in between). Review and analysis of audit trail records can lead to the detection of unauthorized or otherwise unacceptable system activity. See also **Log on** and **Security audit**.

Authentication- The act of verifying a user's identity in order to prevent unauthorized use. See also **User, Biometrics, Digital certificate, Digital signature, Log on,** and **Password**.

Back door- A mechanism for circumventing or disabling system security as purposefully devised and included by system designers. Back doors are presumably "justified" because they offer system access to technicians and other administrators who have been made aware of the deliberate flaw. Unfortunately, searching for (and finding) back doors is a common and fairly effective attack technique used by uninvited system hackers as well. See also **Access, Vulnerability,** and **Hacker**.

Back up- (Verb) To make a copy of a file or program for the purpose of restoring the data if the masters were to be lost, damaged, or otherwise unavailable for use.

Backup- (Noun) A copy of a master file or program. To be most effective from a security standpoint, back-up files are frequently stored at off-site locations. See also **Master file** and **Off-site storage**.

Biometrics- The use of biological characteristics (e.g., retinal patterns, fingerprints, and voice properties) to uniquely identify a person. These measurements can then be used to authenticate computer users. See also **Authentication, User**, and **Voice recognition**.

Bit- A *b*inary dig*it*. The smallest unit of computer memory, eight of which constitute a byte. The value of each bit, as limited by the "binary" code read by computers, is either 0 or 1. See also **Byte, Megabyte (MB),** and **Memory**.

Browser- See **Web browser**.

Bug- A programming error that prevents software from performing as designed and anticipated. See also **Computer program** and **Software**.

Byte- Eight bits. The amount of computer memory needed to store one character (i.e., a number, letter, or symbol). See also **Bit, Megabyte (MB),** and **Memory**.

Cables (a.k.a. cabling)- An assembly of insulated electronic conductors used to connect electrical equipment (e.g., peripheral equipment to a computer). See also **Wireless**.

CD- See **Compact disc**.

CD-ROM (Compact Disc-Read Only Memory)- An optical disk capable of storing large amounts of embedded electronic programs or files that can only be *read* from the disk (i.e., data can not be *written to* the disk after it has been produced). Unlike diskettes, CD-ROMs can be read by any type of computer with a CD-ROM disk drive. See also **Compact disc** and **Diskette**.

Central processing unit (CPU)- The main chip that controls the operation of the rest of the computer (i.e., the computer's "brain," where instructions are processed and information flow is managed). In a personal computer, a microprocessor serves as the CPU. See also **Microchip** and **Microprocessor**.

Certificate- See **Digital certificate**.

Certificate authority- A "trusted" third-party entity that issues digital certificates to individuals or organizations. The digital certificates are then used to create digital signatures and other security mechanisms. By issuing a digital certificate, the certificate authority guarantees that the recipient of the unique identifier is who he or she claims to be. See also **Digital certificate** and **Digital signature**.

Chip- See **Microchip**.

Client- The computer (user) in a client/server network that requests the files or services. The computer that supplies the services is the server. See also **Thin client, Server,** and **Client/server network**.

Client/server network- A network configuration in which all users access files stored on a central computer or several central computers. Each central computer is a server, and each user (actually each user's computer) is a client. See also **Client, Thin client, Server, Peer-to-peer network,** and **Network**.

Code- 1. (Noun) A familiar, if not precise, expression for a computer program, especially in its developmental form. 2. (Verb) A colloquial term for writing a computer program (i.e., a term for programming). See also **Computer program** and **Computer programmer**.

Cold site- An off-site location that includes all files, data, and software (but *not* hardware) necessary for resuming critical systems after an emergency has rendered an organization's primary site inoperable. Because some time is usually required to purchase and install the missing hardware, cold sites are plausible contingency plans only when a delay in restoring operations is acceptable. On the positive side, maintaining a cold site also delays the expense of purchasing the hardware until it is absolutely necessary (i.e., if, and only if, there is an emergency that damages or destroys the organization's primary work site). See also **Off-site**, **Critical system, Contingency plan,** and **Hot site**.

Compact Disc- A 4.75 inch optical disk that can store computer files and data, audio signals, video images, and other digital files. Compact discs are frequently published in a read-only format (which are then called CD-ROM for Compact Disc-Read Only Memory), but when not configured as such, can be written to as well. See also **CD-ROM**.

Computer- An electronic device that can be programmed with instructions for storing, retrieving, and processing data. A computer is composed of hardware and software, and can exist in a variety of sizes and configurations. See also **Mainframe computer, Minicomputer, Personal computer, Computer program, Computer type, Hardware, Software,** and **Data**.

Computer program- Electronic instructions for a computer. See also **Computer, Software, Operating system software, Application software, Administrative software, Instructional software,** and **Code**.

Computer programmer- A person who writes computer programs (i.e., a person who writes instructions for computers). See also **Computer program** and **Code**.

Computer type- The classification of a computer according to its storage and computing capacity, the number of users that it can support, the variety of input and output options it offers, and its physical size. Three major types of computers are mainframe computers, minicomputers, and personal computers (i.e., microcomputers). See also **Mainframe computer, Minicomputer, Personal computer,** and **Computer.**

Computerize- (1) To equip with computers, (2) to control by means of computers, or (3) to input and store in a computer. See also **Computer.**

Confidential information- Private information about an individual that is protected by organizational policy or law (such as the Family Education Rights and Privacy Act (FERPA). See also **Directory information, General information,** and **Sensitive information.**

Contingency plan- A prepared plan that details an organization's anticipated response to potential emergency situations. The purpose of a contingency plan is to minimize the amount of planning necessary once an organization and its staff find themselves in an emergency situation (e.g., a fire, earthquake, or flood); instead, they can refer to, and enact, the *pre-planned* list of activities already identified as necessary for protecting people, salvaging systems, and limiting damage. Well-designed contingency plans *specify* individual staff roles and responsibilities during an emergency. See also **Recovery plan**.

Conversion- The task of migrating data from an existing computer or software system (or from paper files) to a new system.

Countermeasure- A step planned and taken in opposition to another act or potential act, including the introduction of security procedures to a system in order to minimize vulnerabilities and neutralize threats. See also **Asset, Attack, Risk, Threat, Vulnerability,** and **Risk Assessment**.

CPU- See **Central processing unit**.

Critical system- A computer, network, system or component that is absolutely essential (i.e., critical) to the operation of an information system. See also **General system** and **System**.

Data- Raw information that lacks the context to be meaningful (e.g., "34" is data because it has no meaning unless some context is provided; "34 *degrees Fahrenheit*" has meaning and therefore becomes information). The terms "data" and "information" are often used to differentiate between computer-read (i.e., data) and human-read (i.e., information) figures and text. See also **Information**.

Database- A large collection of data that is developed and maintained for quick searching and retrieving. See also **Data** and **Database software**.

Database software- Computer programs designed to store large amounts of data and allow for quick and efficient searching, retrieving, sorting, revising, analyzing, and ordering. There are two common types of databases, flat file databases and relational databases. See also **Data, Computer program, Software, Administrative software,** and **Application software**.

Decryption- The process of translating an encrypted file back into its original unencrypted form via the use of a matching decryption key. See also **Encryption** and **Key**.

Degauss- To demagnetize. Disks and other electronic storage media are degaussed in order to completely remove magnetically encoded data. Degaussing is necessary because simply erasing files does not, in most cases, ensure complete data removal.

Digital certificate- An attachment to an electronic transmission that allows the recipient to authenticate the identity of the sender via third party verification from an independent certificate authority. Digital certificates are used to identify encryption and decryption codes between message senders and recipients. See also **Certificate authority, Digital signature, Encryption, Decryption,** and **Authentication**.

Digital signature- A code attached to an electronic message that is used to verify that the individual sending the message is really who he or she claims to be—much in the same way that a written signature identifies the sender of a piece of written correspondence. To be effective, digital signatures must be unique and must, therefore, be protected from theft and forgery. See also **Certificate authority** and **Digital certificate**.

Directory information- Information about an individual that can legally be made public (e.g., name, street address, and telephone number). See also **Confidential information, General information,** and **Sensitive information**.

Disk- A round plastic magnetic device on which computer programs and data are saved. There are three main types of disks: hard disks (maintained inside the computer on the hard drive), diskettes (e.g., floppy disks), and compact discs (e.g., CD-ROM). See also **Hard disk, Diskette, Compact disc, CD-ROM, Disk drive,** and **Hard drive**.

Disk drive- A device that reads and stores data on a disk. The drive may be permanently installed inside the computer (i.e., a hard drive that reads a hard disk), or contain a slot for entering a diskette or compact disc from outside the computer. See also **Disk, Diskette, Hard disk, Compact disc, CD-ROM,** and **Hard drive**.

Disk label- See **Label**.

Diskette- A thin, flexible, plastic disk on which computer programs and data can be saved outside of a computer. The two types of diskettes are 3.5 inch disks that come in a hard plastic case and 5.25 inch disks that come in thin, pliable, cardboard-like cases and are therefore referred to as floppy disks. See also **Disk** and **Disk drive**.

Download- The act of transferring data or files between computers or systems. Downloading is *sometimes* distinguished from uploading by the direction of the file/data transfer. Downloading refers to transfers from a larger to smaller system or from a remote system to a local system.

Drill- See **Security drill**.

Drive- See **Disk drive** and **Hard drive**.

Dumb terminal- A unit composed of a monitor and a keyboard that connects to a remote computer for its processing power. See also **Monitor** and **Keyboard**.

E-mail- Electronic messages, typically addressed as person-to-person correspondence, that are transmitted between computers and across networks.

Electronic data interchange (EDI)- The exchange of routine education (and business) information transactions in a computer-processable format.

Encryption- The process of translating a file into an apparently unintelligible format (i.e., to encode it) via the use of mathematic algorithms or other encoding mechanisms. In general terms, the recipient of an encrypted message must possess a matching key to decrypt and read the message. See also **Decryption** and **Key**.

Ethical standards- Guidelines for appropriate behavior based on the recognized standards of a profession or group (e.g., ethical standards of the workplace forbid displays of insulting and insensitive messages).

File- In technology systems, a file is a block of data stored on a magnetic medium such as a floppy disk, hard disk, or tape. A file may contain a computer program, a document, or other collections of data and information.

Firewall- An electronic boundary that prevents unauthorized users and/or packets of data or information (e.g., files and programs) from accessing a protected system.

Floppy disk- See **Diskette**.

Freeware- Software that, while available free of charge, is still protected by a copyright and, therefore, is subject to applicable copyright laws. The person who retains the copyright for a piece of software maintains all distribution authority and can choose to charge for the product at any time. See also **Computer program** and **Software**.

Functional specifications- A document that details the desired or expected capabilities of a computer or network (i.e., the system functions and software functions). Functional specifications are best determined through methodical analysis, referred to as a needs assessment, which, when complete, results in a formal needs statement. See also **System functions, Software functions, Needs assessment,** and **Needs Statement**.

Functions- See **Software functions** and **System functions**.

Gateway- An electronic device that allows two different computer or networks to connect (i.e., it "translates" between networks that use different protocols). See also **Interface** and **Protocol**.

General information- Information or data that is useful, but not (1) critical to an organization's mission, or (2) of a confidential or sensitive nature. See also **Confidential information, Directory information,** and **Sensitive information.**

General system- A computer, network, system or component that, while useful, is *not* critical to the operation of an information and technology system. See also **Critical system** and **System**.

Goal of Security- See **Security goal**.

Hacker- An unauthorized user who attempts to access a system and its information.

Hard disk- A device, usually constructed of rigid aluminum or glass, on which computer programs and data are saved. A hard disk is most often permanently connected to the computer's hard drive, although removable hard disks are available. Data is transferred to and from the hard disk by magnetic heads. See also **Disk** and **Hard drive**.

Hard drive (a.k.a. hard disk drive)- A device used to store programs and data to (and read from) a computer's "permanent" hard disk. See also **Disk** and **Disk drive**.

Hardware- Computer equipment that can be touched, including the computer case and peripheral equipment (e.g., monitor, keyboard, mouse, and printers) that is attached to the computer. See also **Peripheral equipment, Monitor, Keyboard, Mouse, Printer,** and **Software**.

Help desk- A source from which computer, network, or software users can receive assistance. Access to a Help desk is usually offered to users via telephone, fax, or e-mail.

Homepage- The first page (i.e., the opening screen) of a website. See also **World Wide Web (WWW)**.

Hot site- An off-site location that includes all resources (including files, data, software, and hardware) necessary for resuming critical systems after an emergency has rendered the organization's primary site inoperable. A hotsite should require little to no delay in restoring operations because all resources are maintained in a ready state. See also **Off-site, Critical system, Contingency plan,** and **Cold site**.

Information- Data that are meaningful (i.e., they are presented in a context that allows them to be read by a human as opposed to being read by a computer). See also **Data**.

Instructional software- Computer programs that allow students to learn new content, practice using content already learned, and/or be evaluated on how much content they currently know. These programs allow teachers and students to demonstrate concepts, perform simulations, and record and analyze data. Sometimes application software such as database programs and spreadsheets can also be used within the instructional context to help analyze and present data and information. See also **Computer program, Software, Administrative software,** and **Application software**.

Integrated Services Digital Network (ISDN)- An international set of telecommunication standards that allow voice, video, and data to be digitally transmitted over wire or optical fiber lines.

Interface- A shared boundary where independent systems meet. In computer systems, the term "interface" commonly refers to the mechanism through which a user communicates with a computer or network (e.g., via a monitor, keyboard, or mouse). It also refers to those connections that enable communication and exchanges of data to take place between separate systems. See also **Gateway**.

Internet- A global "network of networks" that is used by the general population, including educators, students, government, business, and a host of other individuals and organizations to communicate electronically. See also and **World Wide Web (WWW)**.

Internet Service Provider (ISP)- An organization that provides access to the Internet. Commercial providers, nonprofit organizations, and schools can serve as ISPs. See also **Internet**.

Intranet- A localized network of computers used to communicate electronically.

ISDN- See **Integrated Services Digital Network**.

Key- A secret value (usually attached to a mathematical algorithm) that is used to generate unique encryption/decryption codes. See also **Encryption** and **Decryption**.

Keyboard- A piece of peripheral equipment (analogous to a typewriter) used to enter information and instructions into a computer. In addition to letter keys, most keyboards have number pads and function keys that make computer software easier to use. Keyboards are frequently an important tool in the user-computer interface. See also **Peripheral equipment** and **Interface**.

Label- Information that identifies or describes that to which it is affixed. Printed paper labels are used to identify computer disks, whereas electronic labels can be used to identify electronic files. Labels are also affixed to backup tapes, storage cabinets, and other storage media and containers to identify contents. Proper labeling is an integral part of any effective security system.

LAN- See **Local area network**.

Laptop- A portable personal computer that is small enough to fit on a person's lap (i.e., it weighs less than eight pounds). Laptops are usually capable of being powered by rechargeable batteries. See also **Computer, Personal computer, PC,** and **Macintosh**.

Library- See **Media library**.

Local area network (LAN)- An interconnected system of computers and/or peripheral equipment (e.g., printers) that is confined to a limited area, such as a room, building, or campus, and enables connected users to communicate and share information and resources. See also **Wide area network (WAN)**.

Log on (a.k.a. log in)- To connect to a computer or network, usually through the entry of an acceptable user ID and password (i.e., through appropriate authentication). See also **Access**, **Authentication**, and **Password**.

Logic bomb- A hidden computer program that, once activated, damages or destroys a computer or network (e.g., malicious code programmed to damage files at a certain time on a certain day). A logic bomb technically is *not* a virus because it can only be activated once, whereas a virus can replicate itself or otherwise resurface repeatedly. See also **Computer program** and **Virus**.

Macintosh- A family of personal computers manufactured by Apple Computer. See also **Computer**, **Personal computer**, and **PC**.

Mainframe computer- A computer that serves as central support to many users and has the storage and computing capacity needed for large sets of data and files. Mainframes often store data on large reel-to-reel magnetic tapes that require extensive physical storage space. Mainframe users frequently rely upon dumb terminals or "tubes" to connect to the mainframe. See also **Computer**, **Minicomputer, Personal computer,** and **Dumb terminal**.

Maintenance contract- An agreement with an outside service or agency (e.g., the vendor who sold the equipment) to maintain or repair a computer system (and its peripheral equipment).

Masquerading- Impersonating an authorized user to gain access to a computer or network. One common act of masquerading is to "borrow" someone else's password. See also **Spoofing**.

Master file- An original file from which copies and backups are made. See also **Backup**.

Media library- An on-site location that serves as a repository for archived files and software, and allows for security measures to be concentrated and even intensified. Note that a media library is not a substitute for off-site storage of backups. See also **Off-site storage.**

Megabyte (MB)- The amount of computer memory needed to store 1,048,576 characters (which is roughly equivalent to a novel of average length). Megabytes are used to describe the amount of memory on a diskette, hard disk, or in random access memory (RAM). See also **Bit**, **Byte,** and **Memory**.

Megahertz (MHZ)- A measure of the clock speed of a central processing unit (CPU) expressed in millions of cycles per second. See also **Central processing unit (CPU)**.

Memory- In technological terms, the location and medium of data storage within a computer. See also **Storage media** and **Random access memory (RAM)**.

Microchip- A tiny piece of silicon (actually usually, *but not always*, silicon) on which computer circuitry has been manufactured. A microchip, or "chip," is an integral piece of computer hardware and can contain the circuitry for the central processing unit, memory (including random access memory), or other important operations. See also **Microprocessor**, **Central processing unit (CPU)**, and **Hardware**.

Microcomputer- See **Personal computer**.

Microprocessor- The microchip that is responsible for a computer's logical operations. The microprocessor serves as the central processing unit (CPU) in a personal computer. See also **Microchip** and **Central processing unit (CPU)**.

Minicomputer- A stand-alone computer system that generally supports anywhere from five or six to a few hundred users simultaneously. Traditional minicomputers are now often being replaced by client/server networks and peer-to-peer networks. See also **Computer, Personal computer, Mainframe computer**, and **Computer type.**

Modem- Short for "**mo**dulator/**dem**odulator." A device that allows a computer to connect to a telephone line in order to communicate with another computer or network (i.e., it allows for remote access). It translates analog signals to digital signals on the way into the computer, and digital signals to analog signals on the way out of the computer. Modems may be internal or external to the computer case. Modems are classified according to the speed at which they send and receive data. See also **Remote access** and **Peripheral equipment**.

Monitor- A piece of peripheral equipment (analogous to a television screen) that receives video signals from a computer and displays the information (e.g., text and graphics) for the user. A monitor is frequently an important tool in the user-computer interface. See also **Peripheral equipment** and **Interface**.

Mouse- A hand-held piece of peripheral equipment that is rolled across a flat surface (e.g., on a desk) in order to provide direction to a computer. A mouse is frequently an important tool in the user-computer interface. See also **Peripheral equipment** and **Interface**.

Multimedia- A computer capable of utilizing more than one communication medium (e.g., audio *and* video).

Need-to-Know- A legal designation that indicates whether an individual has a legitimate educational reason for accessing confidential information. Also, a security principle that states that a system user should only be granted access to those components of the system (and its information) that he or she actually needs to perform his or her job.

Needs assessment- The process of determining the system functions and software functions that an organization or user will require of a computer or network (i.e., what the system will be "needed" to do). The product of a needs assessment is initially a list of functional specifications and, ultimately (when completed and combined with the system's technical requirements), a needs statement. See also **System functions, Software functions, Functional specifications, Technical requirements,** and **Needs statement**.

Needs statement- A description of the functional specifications, technical requirements, and security standards that dictate the selection of a technology solution. Accurate needs statements usually require input from a range of potential users and are the product of a needs assessment. See also **Functional specifications, Technical requirements,** and **Needs assessment**.

Network- A group of computers (technically two or more) connected to each other to share software, data, files, and peripheral equipment. Also, the hardware and software needed to connect the computers together. See also **Local area network (LAN), Wide area network (WAN), Client/server network, Peer-to-peer network, Intranet, Internet,** and **World Wide Web (WWW)**.

Node- A point of access on a network (i.e., a point of connection). See also **Access** and **Network**.

Off-site- A location other than an organization's primary work site or place of business. See also **Off-site storage**.

Off-site storage- A location for the storage of backup files that is physically independent of the primary site of file use. The purpose of off-site storage is to decrease the likelihood of a single catastrophic event damaging or destroying both master and backup files. For example, if a fire were to break out in a building, it is conceivable that the entire structure could be destroyed. If backup files were maintained in that building, they would probably be lost with the originals; but if the backup files were at a different location (i.e., in off-site storage), they would be much more likely to survive the event. See also **Off-site, Cold site, Hot site, Backup,** and **Master file**.

On-line- The status of being connected to a computer or network or having access to information that is available through the use of a computer or network. See also **Access** and **Remote access**.

Operating system software- The electronic instructions (e.g., Windows 95, Mac OS, Unix, and Novell NetWare) that control a computer and run the programs. Operating system software is usually specific to a particular type of computer. See also **Computer program, Software,** and **Application Software**.

Password- A secret sequence of letters, numbers, or symbols that enables a user to authenticate him- or herself to a secured computer or network. Passwords can be established by a system administrator or by the individual user. Effective password systems require that each user protect his or her password from being disclosed to anyone. See also **Authentication** and **Log on**.

PC- A term which should refer to any type of personal computer (e.g., a Macintosh or IBM-compatible) but has become synonymous with IBM-compatible personal computers. There are quite literally hundreds of brands of IBM-compatible computers (e.g., Compaq, Dell, and Packard Bell personal computers). See also **Computer, Personal computer,** and **Macintosh.**

Peer-to-peer network- A network configuration in which each user stores files on his or her own computer for other network users to access. See also **Client/server network** and **Network**.

Pentium- The fifth generation (hence the name *Pentium*) of the Intel microprocessor. See also **Microprocessor** and **Central processing unit (CPU)**.

Peripheral equipment- Any of a variety of devices that are attached to a computer, including monitors, keyboards, modems, printers, scanners, and speakers. See also **Monitor, Keyboard, Modem,** and **Printer**.

Personal computer (a.k.a. Microcomputer)- A "small" computer (no larger than a desktop by definition) that uses a microprocessor (i.e., a microchip that serves as the central processing unit) to run the computer. Personal computers are generally used by only one person at a time (i.e., the user), but can be networked to communicate with other personal computers, mainframes, or minicomputers. This glossary considers both Macintosh and IBM-compatible computers to be Personal Computers. See also **Computer, Macintosh PC, Mainframe computer, Minicomputer,** and **Laptop**.

Platform- The hardware and operating system software that runs application software on a computer. See also **Hardware, Operating system software, Application software,** and **Computer**.

Printer- A piece of peripheral equipment that translates electronic signals from a computer into words and images on paper. Common types of printers include dot matrix, ink jet, laser, impact, fax, and pen and ink devices; many are capable of producing either black-and-white or color images. See also **Peripheral equipment**.

Program- See **Computer program**.

Programmer- See **Computer programmer**.

Protocol- The set of technical and procedural standards and rules that govern network and computer communication and data exchange. See also **TCP/IP** and **Electronic data interchange (EDI)**.

Random access memory (RAM)- The working memory of a computer (i.e., the microchips on which data is temporarily stored while a computer is on and working). See also **Memory**.

Recovery plan- A detailed program for regaining first an organization's critical systems and then its general systems (i.e., "normal" operations) after a disaster. As with all contingency planning, recovery plans should be prepared in advance of any such occurrence. They should specify individual roles and responsibilities for performing planned responses, and be coordinated with other contingency planning and emergency response efforts. See also **Contingency plan**.

Release- An intermediate edition of a computer program. Releases are usually offered when minor changes or bug-fixes have been made to the previous edition of the software. Releases are designated by a whole number (denoting the version) followed by a decimal number indicating the new release (e.g., Upgrade 2.1). See also **Computer program, Software, Version,** and **Upgrade**.

Remote access- The act of accessing a computer or network from a location that is removed from the physical site of the computer or network. Remote access is often accomplished via the use of a modem. See also **Access** and **Modem**.

Resources- See **Technology resources**.

Risk- In information and technology security, a risk is any hazard or danger to which a system or its components (e.g., hardware, software, information, or data) is subjected. See also **Asset, Attack, Countermeasure, Threat, Vulnerability,** and **Risk Assessment**.

Risk assessment- The process of identifying: (1) all assets an organization possesses, (2) all potential threats to those assets, (3) all points of vulnerability to those threats, (4) the probability of potential threats being realized, and (5) the cost estimates of potential losses. Risk assessment enables an organization to at least consider the range of potential threats and vulnerabilities it faces, and is the first step in effectively securing an information and technology system. See also **Asset, Attack, Countermeasure, Risk, Threat,** and **Vulnerability**.

Rogue programming- See **Logic bomb, Trojan horse, Virus,** and **Worm**.

Screen saver- A computer program that automatically displays a moving image or pattern on a monitor screen after a pre-set period of inactivity. Screen savers were originally designed to prevent a fixed image from being "burned" into the phosphor of the monitor screen, but also afford an additional security function as well—the displayed image or pattern serves to shield screen content from passersby who could otherwise see information shown on the monitor screen. Many screen savers now offer password protection that, while far from foolproof, further deters casual unauthorized viewing of monitor displays. See also **Monitor.**

Security audit- A methodical examination and review of system and user activity. See also **Audit trail**.

Security drill- Repetitive instruction or training designed to establish security concepts and procedures within an organization and its staff.

Security goal- The primary goal of any information and technology security system is to protect one's information and system without unnecessarily limiting its utility for authorized users and functions. See also **Trusted system**.

Security policy- Clear, comprehensive, and well-defined plans, rules, and practices designed to protect and regulate access to an organization's system and the information that comprises it. Security policy describes the ideal status toward which all organizational security efforts should lead.

Security signature- See **Digital signature**.

Sensitive information- Information or data which, if lost or compromised, might negatively affect the owner of the information or require substantial resources to recreate. See also **Confidential information, Directory information,** and **General information.**

Sequence numbering- The use of embedded number patterns within a transmitted message to verify the integrity of file or data exchange. If the sequence of numbers in a received message is not consistent with the sequence in the sent message, it is possible that the message was tampered with or has otherwise lost its integrity.

Server- The computer in a client/server network that supplies the files or services. The computer (user) that requests the services is the "client." See also **Client, Thin client,** and **Client/server network**.

Signature- See **Digital signature**.

Software- Programs that tell a computer what to do. See also **Computer program, Application software, Administrative software, Instructional software, Operating system software, Antivirus software,** and **Hardware**.

Software features- Those attributes offered by a particular piece of software that make it easy and effective to use (e.g., a "spell check" function in word processing software). See also **Software**.

Software functions- The tasks, activities, or operations that a piece of software is intended to perform. See also **Software, Functional specifications, Needs assessment,** and **System functions**.

Spoofing- An intentional act of misrepresentation in which an authorized user is tricked into thinking that he or she is communicating with another authorized user or site (but is not). See also **Masquerading**.

Storage media- Any of a variety of agents or mechanisms for storing electronic data or files, including disks, tapes, and compact discs. See also **Disk, Diskette, Compact disc, Tape, Zip drive,** and **Memory**.

Surfing- The act of exploring locations and browsing contents of World Wide Web sites on the Internet. See also **Web browser**.

System- A group of elements, components, or devices that are assembled to serve a common purpose. In a technological system, this refers to all hardware, software, networks, cables, peripheral equipment, information, data, personnel, and procedures (i.e., all technology resources) that comprise a computer environment. See also **Hardware, Software, Network, Cables, Peripheral equipment, Information, Data, Technology resources, Critical system, General system,** and **System functions**.

System functions- A list of the specific capabilities a computer or network should be able to perform (or staff should be able to do when using the system). Examples of possible functions include storage and retrieval capabilities, calculation and processing capabilities, reporting and output capabilities, and telecommunications capabilities. See also **System, Functional specifications, Needs assessment,** and **Software functions**.

Tape- A storage medium that is both "readable" (i.e., it can be read from) and "writable" (i.e., it can be written to). Tape was a primary storage method for early computers and systems, but has been replaced by disks, compact discs, and other less bulky media. Tape is still frequently used as a medium for making backups (e.g., backup tapes). See also **Storage media**.

TCP/IP (Transmission Control Protocol *over* Internet Protocol)- The *de facto* standard communications protocol used for networking. See also **Network** and **Protocol**.

Technical requirements- Straightforward statements that describe the necessary parameters of a technology solution. These parameters should address topics such as: the number of people who will use the system at a single time; where users are located; the numbers and types of transactions that need to be processed; and the types of technology components that need to interact. See also **Software functions**, **System functions,** and **Needs assessment**.

Technical support staff- Those persons who support and maintain an information system once it has been established. See also **Technology resources**.

Technology resources- The hardware, software, networks, and other equipment (in combination with personnel and financial resources) that can be dedicated to the implementation of a technology solution. See also **Technical support staff** and **System**.

Telecommuter- An individual who works at home or at another location that is physically removed from a place of employment via the use of technology (e.g., computers, modems, and fax machines). See also **Remote access**.

Thin client- A networking system in which the client (i.e., the user's computer) in a client/server network handles very little of the processing because the majority of processing is managed by the server. See also **Client**, **Server, Client/server network,** and **Network**.

Threat- Any actor, action, or event that contributes to the risk of an organizational asset. See also **Asset**, **Attack, Countermeasure, Risk, Vulnerability,** and **Risk Assessment**.

Time stamp- The act of recording the date and time within a transmitted message to verify the integrity of file or data exchange. If the date and time of message receipt varies with the date and time of transmission beyond an acceptable period of delivery, it is possible that the delay signifies that the message was intercepted in transit (or has otherwise lost its integrity).

Trojan horse- A type of programmed threat (i.e., a virus) that presents itself as an apparently useful function (e.g., the "thesaurus" in a word processing application) but actually conceals an unauthorized program designed to damage the system or the information it contains. See also **Threat** and **Virus**.

Trusted system- An information and technology system that, while not invincible, can generally be "trusted". Since no system is foolproof, a trusted system is the ideal security state. See also **Security goal** and **System**.

Upgrade- 1. (Verb) The act of installing a revised or improved (i.e., newer) version or release of a piece of software on a computer or system. 2. (Verb) To add memory or new equipment to an existing computer or network. 3. (Noun) A revised or improved product (i.e., software or hardware). See also **Release, Version, Software, Memory, Random access memory (RAM),** and **Hardware**.

User- In information and technology systems, a user is a person who accesses a system. Education organization users typically include (1) instructional staff who provide instruction or perform instructional management tasks using technology and (2) administrative staff who use technology to manage the routine and non-routine administrative activities of an organization as efficiently as possible. Students, parents, and community members can also be users. See also **Access** and **System**.

Version- A major edition of a computer program. The version number changes when a software developer makes major alterations to the software (e.g., significant new features are added). The version number is a *whole* number following the name of the software, in contrast to the release number, which is the *decimal* number after the version number. For example, when Software 2.0 undergoes minor changes, it could be *re-released* as Software 2.1. When it later undergoes significant revamping, the new *version* would be Software 3.0. See also **Computer program, Software, Release,** and **Upgrade**.

Virus- A computer program that destroys data, unnecessarily ties up resources, or otherwise damages a system. Viruses are often able to replicate themselves and can therefore be passed from one computer or network to another via file transfers (analogous to how a biological virus is passed from one host to the next). Viruses are combated by a variety of security techniques, most notably through the use of antivirus software and virus scanners. See also **Antivirus software, Virus scanner, Threat, Trojan horse,** and **Worm**.

Virus scanner- Software designed specifically to search files and disks for the presence of a virus. See also **Software, Virus, Antivirus software, Trojan horse,** and **Worm**.

Voice recognition- The conversion of spoken language into a digital format by a computer. Voice recognition can be used as a method of user identification and authentication. See also **Biometrics** and **Authentication**.

Vulnerability- A point within an information or technology system that is susceptible to attack from a threat. See also **Asset, Attack, Countermeasure, Risk, Threat,** and **Risk Assessment**.

WAN- See **Wide area network**.

Web- See **World Wide Web (WWW)**.

Web browser- Software that allows a user to locate, view, and access information from World Wide Web sites (on the Internet) via the use of a graphical interface. See also **Surfing.**

Wide area network (WAN)- An interconnected system of computers and networks (including local area networks) that surpasses local area networks in scope (e.g., WANs can span building to building, city to city, across the country, and internationally). These data communications linkages (e.g., dedicated lines and radio waves) are designed to allow large numbers of users to communicate and access information. See also **Local area network (LAN)**.

Wireless- A network system in which there is no physical connection between two pieces of equipment (i.e., instead of a wire or fiber optic links connecting computers, they communicate via radio waves). See also **Cables** and **Network**.

World Wide Web (WWW)- A network that offers access to websites all over the world using a standard interface for organizing and searching. The WWW simplifies the location and retrieval of various forms of information including text, audio, and video files. See also **Surfing** and **Homepage**.

Worm- A computer program that can make copies of itself and spread through connected computers and networks, thereby using up system resources and/or causing other damage. See also **Threat** and **Virus**.

Write-protect- Any of a variety of hardware or software mechanisms that prevent data from being written to a disk or other storage media.

WWW- See **World Wide Web**.

Zip drive- A Zip drive is able to store 25 megabytes to 100 megabytes of data onto removable cartridges (depending on the model of the drive), most frequently for the purpose of backing up data. See also **Backup, Disk, Disk drive,** and **Storage media**.

Note that the following resources were consulted during the development of this glossary:

(1) *Computer Currents On-Line Dictionary* on the World Wide Web at http://www.currents.net/resources/dictionary .

(2) *Inc. Online on Business Technology* (A World Wide Web On-Line Dictionary, copyrighted by the Goldhirsh Group, 1998) at http://www.inc.com/technology/learn/glossaries.html

(3) Russell, D. and Gangemi, G.T. (1991). *Computer Security Basics*. Sebastopol, CA: O'Reilly & Associates.

(4) U.S. Department of Education, National Center for Education Statistics. (1997). *Technology @ Your Fingertips*, NCES 98-293. Washington, DC: Government Printing Office or at http://nces.ed.gov/pubs98/98293.pdf

(5) Whatis.com, Inc. (A World Wide Web On-Line Dictionary) at http://whatis.com

Index

acceptable use policy - see *policy* and *security agreements*
access - 28, 85, 88, see also *user access security*
account - see *user account*
account management - 50
accountability - 4, 31-33, 50
acquisition (software) - 80
airport security - 60
application software - 70, 77
appropriate use policy - see *policy* and *security agreements*
antivirus - 49
asset - 12, 14, 67
attack - 16, 40
audience (document) - 4
audit - 45
authentication - 69, 81, 86, 88, 90, 91, 101
auxiliary power - 61
availability (information) - 67
backups - 47-49, 70-72, 79, 82
biometrics - 70, 88
breach - see *security breach response planning*
browser -100
building and room construction - 57
bug - 49
cabling - 59, 91
call-back system- 91
certificate authority - 101
climate - 58
cold site - 43
complete backup - 48
Computer Emergency Response Team (CERT) - 99
confidential information - 3, 11, 28, 62, 100
confidentiality - 67
consortia - 30
contingency planning - 40, 42-44
cost/benefits - 11, 19, 22-24
countermeasure - 12-13, 16, 22-23, 56
  information security - 69-73
  network (internet) security - 100-101
  physical security - 57-62
  software security - 78-82
  user access security - 87-92
critical facilities - 57
critical system - 19, 29, 59, 79
data - 67, 73
data life cycle - 73
decryption - 68, 101, 102
degaussing - 73
design reviews - 80
development (software) - 80
dial-up communications - 69, 92
digital certificate - 101
digital signature - 101
discipline - 41
disposal - 62, 73
documentation - 70, 79, 81
doors - 57
drill - 45, 52
e-mail - 69
electrical system - 61
encryption - 68, 69, 89, 91, 100, 101, 102
enforcement - 32
fax machines - 61
Family Educational Rights and Privacy Act (FERPA) - 3, 67, 110
fire - 58
firewall- 92, 100
general information - 19
general system - 19, 59
goals (security) - 7
goals (training) - 109
hot site - 43
humidity - 58
incremental backup - 48
information - 3, 14-15, 20, 67, 73
information security - 22, 67-76
installation (software) - 80
insurance - 14
integrity (information) - 67
intentional threat - 15, 21, 57, 68, 78, 87, 99
internet - 50, 92, 97, 98, 100
internet security - see *network (internet) security*
intranet - 98, 102
job-alike training - 109
key (encryption) - 69, 101, 102
key identifiers - 70
labeling - 60, 62, 71
laptop computer - 60
locks - 57
log-on (log-in and log-off) - 50, 90
logs - 50, 71
mail - 62
maintenance contract - 59
management - see *security management*
manager - see *security manager*

manmade threat - 15, 21
media library - 72
modem- 91, 92
monitoring - 50, 69, 80, 86, 88, 89, 91
natural threat - 15, 21, 57, 68, 78
need-to-know - 3, 85
network - 69, 92, 97, 98
network (internet) security - 22, 97-103
node - 91
off-site storage/facility - 43, 49, 79
opening screen - 86
organizational support - 39-40
outlets - 61
output - 61
outsiders - 30, 33, 42, 98, 100
partial backup - 48
password - 69, 86, 88, 89
peripheral equipment - 59
personnel - 29, 33, 39, 87, 105
photocopiers - 61
physical security - 22, 55-66
policy - see also *security policy*
  content - 30
  development - 29-34
  implementation - 31
  information security - 68
  network (internet) security - 99
  physical security - 56
  retention - 73
  software security - 78
  tone - 30
  user access security - 87
portable equipment - 60
power - 61
printers - 61
programming - 78, 79
proprietary software - 79
public/private key encryption - 102
purpose (document) - 4
recovery planning - 42
release - 49
remote access - 86, 91
repair - 59
response planning - see *security breach response planning*
retention policy - 73
risk - 3, 12, 14, 17
risk assessment - 11-25, 29, 55, 107
scanners - 61
school records (use of) - 1, 20
screen saver - 91
secure sockets layer (SSL) - 100
security agreements - 33, 56, 92
security breach response planning - 41
security management - 31, 37-53
security manager - 37-53
security policy - 27-35, 37, 39, see also *policy*
sensitive information - 19, 29, 68, 70, 72, 91
sequence numbering - 101
server - 100
shipping - 62, 70
single key encryption - 102
software - 49, 77
software security - 22, 77-84
static electricity - 61
storage - 71, 79
structural protection - 57
support - see *organizational support*
surge protectors - 61
system administrator - 38
system administrator privileges - 50
system use - 37, 50
table-design applications - 70
tapes (backup) - 71, 73
telecommuters - 86
temperature - 58
testing - 44, 45-46, 52, 71, 78, 79, 82
theft - 60
threat - 12, 15, 20-21, see also *natural threat*, *manmade threat*, *intentional threat*, and *unintentional threat*
  information - 68
  network (internet) - 99
  physical - 57
  software - 78
  user access - 87
time stamp - 101
training - 22, 31, 38, 80, 105-114
transmissions - 69, 91, 100
trusted system - 8, 17, 109
unintentional threat - 15, 21, 57, 68, 78, 87, 99
uninterruptible power source (UPS) - 61
update - 49
upgrade - 82
user - 29, 40, 86, 87, 97
user access security - 22, 85-96
user account - 50, 88
value (system/component) - 11, 19
videotape - 59
views applications - 70
virus - 49, 78, 82
vulnerability - 12, 16, 20-21
waste - 62
web - 99, 100
web browser - 100
window - 57
write-protection - 72
x-rays - 60

United States
Department of Education
Washington, DC 20208-5651

Official Business
Penalty for Private Use, $300

Postage and Fees Paid
U.S. Department of Education
Permit No. G-17

Standard Mail (A)

NCES ###